UNIVERSITY OF TURKU

Faculty of Law

RIGHT TO BE FORGOTTEN IN SPENT CRIMINAL CONVICTIONS

Advanced Studies in Law and Information Society

Kamrul Faisal

Master's Thesis

MDP in Law and Information Society

Faculty of Law

University of Turku

March 2020

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin OriginalityCheck service.

UNIVERSITY OF TURKU
Faculty of Law

Faisal, Kamrul: Right to Be Forgotten in Spent Criminal Convictions

Master's Thesis, XVII + 78 pages.
Master's Degree Programme in Law and Information Society (LIS)
March 2020.

ABSTRACT

Individual's past personal data proved to have unimaginable impact on his or her present and the future in particular the spent criminal convicts' faux pas committed in the past might trap oneself to an unchangeable present and the future. This impact is greater in this advanced communication technological era when personal information is just one click away through search engines and potential victims might be reformed sinners, minor offenders, adolescents and prospective employees who want to represent themselves in consistent with the respective societal interests and values. A successful exercise of right to be forgotten, a derivative of data protection privacy right under GDPR can aid in characterizing this aspiration of reintegration through a new inception of reformed life by restricting the access of the concerned information online. Since access to information is an aspect of right to freedom of expression, both need to be weighed against each other to prioritize one in each case. The established concept and jurisprudence of RTBF does not guarantee any spent criminal convict to erase the relevant history permanently, rather only to delink the hyperlinks from the Internet search engines which makes the retrieval difficult. Even, to reach that far, a series of certain balancing principles suffice in motion which need to be evaluated to weigh between RTBF and free expression, such as, whether the process at issues is a lawful or unlawful one, data subject is a public or private figure, and proportional processing or privacy interests in motion. These characteristics make a RTBF application non-exclusive in nature since it cannot be guaranteed to spent convicts as admittedly, it must face the risk of rejection.

Keywords: Data protection, Right to be forgotten, Freedom of expression, Spent convicts, Publication interest, Privacy interest, Internet, GDPR, *Google Spain*.

ACKNOWLEDGEMENT

I would like to express my gratitude to everyone who supported me throughout the thesis work. I am particularly grateful to my supervisor Professor Juha Lavapuro, Faculty of Law, University of Turku, for his splendid supervision, inspiration and valuable guideline as well as feedback during the work. Further gratitude to my family members, friends and everyone else who supported and inspired me during my study.

Table of Contents

BIBLIOGRAPHY

1. Statutes

- General Data Protection Regulation Regulation 2016/679
- Data Protection Directive 95/46/EC
- Charter of Fundamental Rights of the European Union 2000/C 364/01
- European Convention on Human Rights 1950
- Treaty on the Functioning of the European Union 2007
- Universal Declaration of Human Rights 1948
- International Covenant on Civil and political Rights 1966

2. Books and Publications

- King, Peter, The Life of John Locke: With Extracts from His Correspondence, Journals And Common-Place Books. Creative Media Partners, LLC, 2015, p. 109.
- Rustad, Michael L & Kulevska, Sanna, Reconceptualizing The Right To Be Forgotten To Enable Transatlantic Data Flow. 28 HARV. J.L. & TECH. 2015, pages 349, 353, available at: http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech349.pdf. (accessed on January 20, 2020)
- Rosen, Jeffrey, The Privacy Paradox: Privacy and Its Conflicting Values. Symposium Issue, 64 STAN. L. REV. ONLINE 88, 13 February 2012, page 89, available at: https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/ (accessed on January 20, 2020)
- Reding, Viviane, Privacy Matters: Why the EU Needs New Personal Data Protection Rules. 30 November 2010, available at: http://europa.eu/rapid/press-release_SPEECH-10-700_en.pdf. (accessed on January 20, 2020)
- Maduro, Miguel Pojares, Interpreting European Law: Judicial Adjudication in a Context of Constitutional Pluralism. 1 EUR. J. LEGAL STUD., 2007, pages 138, 146.
- Oster, Jan, Media Freedom as a Fundamental Right. Cambridge University Press, June 2015, pages 69 and 147.
- Draft Report on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data

and on the Free Movement of Such Data. Committee on Civil Liberties, Justice and Home Affairs, COM 0011, 2012, pages 51–52.

- Koops, B. J., Forgetting footprints, shunning shadows: A critical analysis of the 'right to be forgotten' in big data practice. SCRIPTed, 2011, 8:1-28, page 231.
- Blanchette, J-F and Johnson, DG, Data Retention and the Panoptic Society: The Social benefits of Forgetfulness, 18 The Information Society, 2002, pages 33-45.
- Dodge, M and Kitchin, R, Outlines of a World Coming into Existence: Pervasive Computing and the Ethics of Forgetting, 34 Environment and Planning B: Planning and Design, 2007, pages 431-445
- Policy and Research Group of the Office of the Privacy Commissioner of Canada, Online Reputation, what are they saying about me? Discussion Paper, Office of the Privacy Commissioner of Canada, 2016, page 13
- Opinion 2/2017 on data processing at work, Article 29 Data Protection Working Party. WP 249, 8 June 2017, page 3, available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=45631 (accessed on January 7, 2020)
- Rouvroy, A, Réinventer l'Art d'Oublier et de se Faire Oublier dans la Société de l'Information? Version augmentée, 2008, (self-translation) available at: http://works.bepress.com/antoinette_rouvroy/5 (accessed on December 17, 2019)
- Koops, B. J., Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to be Forgotten' in Big Data Practice. Social Science Research Network, 20 December 2011, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986719 (accessed on January 20, 2020)
- Parker, ES. Cahill, Larry and McGaugh, James L., A Case of Unusual Autobiographical Remembering, 12 Neurocase, 2006, pages 35-49, available at: https://www.tandfonline.com/doi/pdf/10.1080/13554790500473680?needAccess=true (accessed on February 18, 2020)
- O'hara, Kieron, Shadbolt, Nigel and Hall, Wendy, A Pragmatic Approach to the Right to Be Forgotten, Global Commission on Internet Governance, Paper Series No. 26, March 2016.
- O'hara, Kieron, The Devil's Long Tail, Oxford, Oxford University Press, 2015.
- Gross, RD. Richard and McIlveen, R. Memory, London: Hodder & Stoughton, 1999.

- Margalit, Avishai, The Ethics of Memory, Cambridge, MA: Harvard University Press, 2002.
- Augé, Marc, Oblivion, Minneapolis: University of Minnesota Press, 2004.
- Siry, Lawrence and Schmitz, Sandra, A Right to be Forgotten? How Recent Developments in Germany May Affect the Internet Publishers in the US. European Journal of Law and Technology 3 (1), 2012, available at: http://ejlt.org/article/download/141/222. (accessed on January 15, 2020)
- Jacobs, James B. and Larrauri, Elena, European Criminal Records & Ex-Offender Employment, University Public Law and Legal Theory Working Papers 532, New York: Oxford University Press, 2015, page 3, available at: https://pdfs.semanticscholar.org/3510/55320fac1899f60dcf14db7c764e39c05230.pdf (accessed on January 15, 2020)
- Larrauri, Elena, Are police records criminal records? Disclosure of criminal information and the presumption of innocence. European Journal of Crime, Criminal Law and Criminal Justice 22, 2014, pages 377-395, available at: https://www.academia.edu/9379880/Are_Police_Records_Criminal_Records (accessed on January 15, 2020)
- Pagallo, Ugo and Durante, Massimo, Legal Memories and the Right to Be Forgotten, Protection of Information and the Right to Privacy- A New Equilibrium? Law, Governance and Technology Series 17, Springer International Publishing, Switzerland, 2014. DOI 10.1007/978/-3-319-05720-0_1,
- Art. 29 Data Protection Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. C-131-12, 4/EN WP 225, 26 November 2014, pages 3, 9, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2014/wp225_en.pdf.
- Lee, Edward, Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten. 49 U.C. Davis L. Rev. 1017, 2016, page 31, available at: http://scholarship.kentlaw.iit.edu/fac_schol/847
- Schechner, Sam, French Privacy Watchdog Orders Google to Expand 'Right to Be Forgotten,' WALL ST. J. 12 June 2015, available at: http://www.wsj.com/articles/french-privacy-watchdog-orders-google-toexpand-right-to-be-forgotten-1434098033. (accessed on January 17, 2020)

- Neville, Andrew, Is it a Human Right to be Forgotten? Conceptualizing the World View, 15 Santa Clara J. Int'l L. 157, 2017, available at: https://digitalcommons.law.scu.edu/scujil/vol15/iss2/2 (accessed on February 18, 2020)
- Roberts, Jeff John, The Right to be Forgotten From Google? Forget it, Says U.S. Crowd. Fortune, 12 March 2015, available at: http://fortune.com/2015/03/12/the-right-to-beforgotten-from-google-forget-it-says-u-s-crowd/. (accessed on January 17, 2020)
- Bernal, Paul Alexander, A Right to Delete? European Journal of Law and Technology 2 (2), 2011, available at: http://ejlt.org/article/view/75. (accessed on January 17, 2020)
- Opinion of Advocate General Jääskinen, Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 13 May 2014, available at: http://curia.europa.eu/juris/document/document.jsf?docid=138 782&doclang=EN (accessed on November 7, 2019)
- Lindsay, David, The 'Right To Be Forgotten' in European Data Protection Law, in Emerging Challenges In Privacy Law, Normann Witzleb et al. eds., 2014, pages 290–337, DOI: https://doi.org/10.1017/CBO9781107300491.019 (accessed on February 17, 2020)
- Clarke, R. Tax File Number Scheme: A Case Study of Political Assurances and Function Creep, 7 Policy (4), 1991.
- Curry, MR. et al. Emergency Response Systems and the Creeping Legibility of People and Places, 20 The Information Society, 2004, page 362.
- Gratton, Eloïse and Polonetsky, Jules, Privacy above all other Fundamental Rights? Challenges with the Implementation of a Right to be Forgotten in Canada, 28 April 2016, available at: https://fpf.org/wp-content/uploads/2016/04/PolonetskyGratton_RTBFpaper_FINAL.pdf (accessed on January 17, 2020)
- Trudel, Pierre, L'oubli en tant que droit et obligation dans les systèmes juridiques civilistes, Unpublished work prepared for the course in cyberlaw, Faculty of Law, University of Montreal, available at: https://pierretrudel.openum.ca/files/sites/6/2016/08/NotesoubliREV-1.pdf (accessed on January 10, 2020)

- Ferrari, Anne, Using Celebrities in Abnormal Psychology as Teaching Tools to Decrease Stigma and Increase Help Seeking. Teaching of Psychology. 43 (4), 2016, pages 329–333, doi:10.1177/0098628316662765
- Coors, Corinna, Headwind from Europe: The New Position of the German Courts on Personality Rights after the Judgment of the European Court of Human Rights. German Law Journal 11 (5), 2010, pages 531–538.
- De Baets, Antoon, A historian's view on the right to be forgotten, International Review of Law, Computers & Technology, 30:1-2, 2016, pages 57- 66, DOI: 10.1080/13600869.2015.1125155, available at: https://doi.org/10.1080/13600869.2015.1125155
- Feinberg, Joel, Philosophy of Law, Limits to the Free Expression of Opinion. Belmont: Calif, 1991.
- Feinberg, Joel and Gross, Hyman, Philosophy of law. Belmont, CA : Thomson/Wadsworth, 1991, pages 138–139.
- Jacobs, James B. and Larrauri, Elena, Are criminal convictions a public matter? The USA and Spain. Punishment and Society 14(1), 2012, pages 3-28.
- Jones, Meg Leta, Forgetting Made (Too) Easy. Communications of the ACM 58 (6), 2015, pages 34-35.
- Foster, Jonathan K. Memory: A Very Short Introduction. London, Oxford University Press, 2008.
- Mayer-Schöenberger, V, Delete: The virtue of forgetting in the digital age, Princeton: Princeton University Press, 2009
- Ricoeur, Paul, La marque du passé, Revue de Métaphysique el de Morale 1, 1998, pages 7-31.
- Reinhardt, Koselleck, Futures Past: On the Semantics of Historical Time, New York, Columbia University Press, 2004.
- Nietzsche, Friedrich, Untimely Mediations, Cambridge Texts in the History of Philosophy. New York: Cambridge University Press, 1997.
- Sartor, Giovanni, The Right to be Forgotten: Dynamics of Privacy and Publicity, L. Floridi (ed.), Protection of Information and the Right to Privacy- A New Equilibrium?, Law, Governance and Technology Series 17, Springer International Publishing Switzerland 2014, DOI 10.1007/978-3-319-05720-0_1.
- Sartor, Giovanni, The logic of proportionality: Reasoning with non-numerical magnitudes. German Law Journal 14, 2013, pages 1419-1457.

- Werro, F. The right to inform v. the right to be forgotten: A transatlantic clash, Liability in the third millennium, eds. A. Colombi Ciacchi, C. Godt, P. Rott, L. j. Smith, Baden-Baden: Nomos, 2009, pages 285-300.
- Weber, R. H. The right to be forgotten: More than a Pandora's box? Journal of Intellectual Property, Information Technology and E- Commerce 2, 2011, pages 120-130.
- Bennett, Steven, The "Right to Be Forgotten": Reconciling EU and US Perspectives. 30 BERKELEY J. INT'L LAW, 2012, pages 161, 169.
- Jacobs, James B. The Eternal Criminal Record. Cambridge, MA: Harvard University Press 2015.
- Article 29 Data Protection Working Party, Opinion 5/2009 on Online Social Networking, 2009, page 6.
- Hildebrandt, M. Profiling and the Identity of the European citizen, M Hildebrandt and S Gutwirth (eds), Profiling the European Citizen, Springer, 2008, pages 303-326.
- Koops, B.J. Law, Technology, and Shifting Power Relations. 25 Berkeley Technology Law Journal, 2010, pages 973-1035.
- Cavoukian, A. Privacy by Design: The Definitive Workshop. A Foreword. 3 Identity in the Information Society 2010, pages 247-251.

3. Case study

- Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, 2014 ECLI:EU:C:2014:317
- CJEU, Joined cases C-92/09 and C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 9 November 2010, para. 48
- CJEU, C-275/06, Productores de Música de Espana (Promusicae) v. Telefónica de Espana SAU, 29 January 2008, para. 68
- ECtHR, 10 March 2009, Times Newspapers Ltd v. the United Kingdom (Nos 1 and 2), CE:ECHR:2009:0310JUD000300203, § 27
- ECtHR, 10 January 2013, Ashby Donald and Others v. France, CE:ECHR:2013:0110JUD003676908, § 34
- ECtHR of 19 February 2013, Neij and Sunde v. Sweden, application No 40397/12, §10
- Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), C-507/17, 24 September 2019, paragraph 46

- Sweden v. Bodil Lindqvist, 2003 E.C.R. I-12992, I-13004-06 (Nov. 6, 2003) Huber v. Germany, 2008 ECR I-09705
- Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy, Case C-73/07, 2008 E.C.R. I-9831, para. 39 (May 8, 2008)
- Társaság a Szabadságjogokért v. Hungary, 37374/ 05, 14 April 2009, paragraph 35
- Österreichische Vereinigung zur Erhaltung, Stärkung und Schaffung v. Austria, 39534/07, 28 November 2013, paragraph 41
- Youth Initiative for Human Rights v. Serbia, 25 June 2013.
- Institut professionnel de agents immobiliers (IPI) v. Englebert, Case C-473/12
- Youth Initiative for Human Rights v. Serbia, 48135/06, 25 June 2013.
- GC, AF, BH, ED v CNIL Case C-136/17, paragraph 25
- Tribunal Supremo (Sala de lo Civil) Oct. 16, 2008 (No. 948); Tribunal Supremo (Sala de lo Civil) Oct,28, 2008 (No. 1013); Tribunal Supremo (Sala de lo Civil) Dec. 23, 2009 (No. 868); Tribunal Supremo (Sala de lo Civil) March 9, 2010 (No. 155); Tribunal Supremo (Sala de lo Civil) Apr. 28, 2010 (No. 264).
- Charleston v New Group Newspapers Ltd [1995] 2 AC 65
- Société TVA inc. v.Marcotte, 2015 QCCA 1118 at 99
- Société Radio-Canada v. Radio Sept-Îles inc., 1994 CanLII 5883 (QC CA).
- Grant v. Torstar Corp., 2009 SCC 61, at para. 105.
- Von Hannover v Germany (No 1) (2005) 40 EHRR 1, at [63].
- NT1 and NT2 v Google and The Information Commissioner, [2018] EWHC 799 (QB)

4. Reports and Online Sources

- Warman, matt, EU Fights 'Fierce Lobbying' to Devise Data Privacy Law. TELEGRAPH (Feb. 9, 2012), available at: http://www.telegraph.co.uk/technology/internet/9069933/EU-fights-fierce-lobbying-todevise-data-privacy-law.html. (accessed on January 5, 2020)
- BBC. 2015. “Sexting Boy’s Naked Selfie Recorded As Crime By Police.” BBC News, September 3, available at: www.bbc.co.uk/news/uk-34136388. (accessed on January 3, 2020)
- ETS (nº 108) http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm. (accessed on January 5, 2020)
- The Digital Universe Decade (2010) available at:

http://www.emc.com/collateral/demos/microsites/idc-digital-universe/iview.htm (accessed 1 Nov 2011).

- Google's Chief Legal Officer, David Drummond, We Need to Talk about the Right to be Forgotten, The Guardian, July 10, 2014. Available at: http://www.unlock.org.uk/policy-issues/policy-cases/case-of-natasha-online-links-hampering-chances-of-promotion/ (accessed on 7 April 2018)
- http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm (accessed on 3 May 2018)
- http://www.unlock.org.uk/unlock-speak-at-ico-policy-conference-the-google-effect-criminal-records-and- the- right-to-be-forgotten/ (accessed on 3 May 2018)
- http://www.unlock.org.uk/unlock-speak-at-ico-policy-conference-the-google-effect-criminal-records-and-the-right-to-be-forgotten/ (accessed on 3 May 2018)
- https://www.theguardian.com/sustainable-business/2015/oct/15/exclude-criminal-records-from-job-applications-companies-urged (accessed on 3 May 2018)
- https://careers.workopolis.com/advice/the-three-things-that-employers-want-to-find-out-about-you-online/ (accessed on 5 May 2018)
- https://christopherstacey.wordpress.com/2015/11/11/the-google-effect-criminal-records-and-the-right-to-be-forgotten/ (accessed on 15 May 2018)
- http://www.unlock.org.uk/policy-issues/specific-policy-issues/google-effect/ (accessed on 15 May 2018)
- http://www.unlock.org.uk/policy-issues/policy-cases/case-of-natasha-online-links-hampering-chances-of- promotion/ (accessed on 15 May 2018)
- https://www.humanrights.gov.au/human-rights-discrimination-employment-basis-criminal-record-0 (accessed 15 May 2018)
- http://www.theguardian.com/media/greenslade/2014/oct/16/freedom-of-speech-google (accessed on 15 May 2018)
- https://careers.workopolis.com/advice/the-three-things-that-employers-want-to-find-out-about-you-online/ (accessed on 16 May 2018)
- http://curia.europa.eu/juris/document/document.jsf?docid=138782&doclang=EN (accessed on 18 May 2019)
- http://www.europarl.europa.eu/meet (accessed on 16 May 2018)
- https://www.priv.gc.ca/information/research-recherche/2016/or_201601_e.asp (accessed 3 June 2019)

- http://curia.europa.eu/juris/showPdf.jsf?text=&docid=48382&pageIndex=0&doclang=en&mode=1st&dir=&occ=first&part=1&cid=361596 (accessed on 14 June 2019)
- http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=1st&dir=&occ=first&part=1&cid=356089 (accessed on 14 June 2019)
- http://eur- lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:62007CJ0073 (accessed on 14 June 2019)
- Simon Mundy, Asia Considers 'Right to be Forgotten' Ruling Prompted by Google, THE FINANCIAL TIMES, (Mar. 12, 2015), available at: http://www.ft.com/intl/cms/s/0/ade889d4-bc0e-11e4-a6d7-00144feab7de.html. (accessed on January 5, 2020)
- Cacciottolo, Mario, The Streisand Effect: When Censorship Backfires. BBC News, June 15, 2012. Available at: http://www.bbc.co.uk/news/uk-18458567. (accessed on January 25, 2020)
- Parkinson, Justin, The Perils of the Streisand Effect. BBC News, July 30, 2014, available at: http://www.bbc.com/news/magazine-28562156. (accessed on January 5, 2020)
- European Commission Memo: Data Protection Day 2014, Full Speed on EU Data Protection Reform. Available at: http://europa.eu/rapid/press-release_MEMO-14-60_en.htm. (accessed on July 17, 2019)
- Japanese Court Orders Google to Halt Search Harassment, JAPAN TIMES, Oct. 10, 2014, available at http://www.japantimes.co.jp/news/2014/10/10/national/crime-legal/tokyo-court-orders-googleremove-search-results-man/#.VlO5Ka6rRE5. (accessed on January 5, 2020)
- Tokyo High Court Overturns Man's 'Right to be Forgotten,' JAPAN TIMES, July 13, 2016, available at: http://www.japantimes.co.jp/news/2016/07/13/national/crime-legal/tokyo-high-court-overturns-mansright-forgotten/#.V6ar2pMrJE4. (accessed on January 5, 2020)
- New DUI Reportability Requirements, California Department of Motor Vehicles, available at:

https://www.dmv.ca.gov/portal/dmv/detail/pubs/dui/reportability/!ut/p/a0/04_Sj9CPykssy0xPLMnMz0vMAfGjzOK9PV1cDT3cDbzdTX0cDRy9PTz8w1zDjNwtjfULsh0VAe_Cq0o!/. (accessed on January 5, 2020)

- Removal Policies, GOOGLE, https://support.google.com/websearch/answer/2744324 (accessed on January 8, 2020)
- Australian Human Rights Commission, Discrimination in Employment On The Basis Of Criminal Record; Article C (Dec. 2004), available at: https://www.humanrights.gov.au/human-rights-discriminationemploymeny-basis-criminal-record#tocC. (accessed on August 7, 2019)
- Michael Douglas, Do We Have The Right To Be Forgotten?, 6:10 TED (2015), available at: http://tedxtalks.ted.com/video/Do-we-have-the-right-to-be-forg (accessed on January 5, 2020)
- Whitney, Lance, Google Hit by More than 144,000 'Right to be Forgotten' Requests. CNET.COM, Oct. 10, 2014, available at: http://www.cnet.com/uk/news/google-hit-by-more-than-144000-right-to-be-forgotten-requests/. (accessed on January 8, 2020)
- Factsheet on the "Right to be Forgotten" Ruling (C-131/12), EUROPEAN COMMISSION, available at: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf. (accessed on January 15, 2020)
- Reding, Viviane, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age, Innovation Conference Digital, Life, Design. Munich, 22 January 2012, available at: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF. (accessed on January 7, 2020)
- Fleischer, Peter, Foggy Thinking About the Right to Oblivion. 9 March 2011, available at: http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html (accessed on January 7, 2020)
- Spauwen, Joran & Brink, Jens van den, Dutch Google Spain Ruling: More Freedom of Speech, Less Right to Be Forgotten for Criminals. Inforrm's Blog, 27 September 2014, available at:

https://inforrm.org/2014/09/27/dutch-google-spain-ruling-more-freedom-of-speech-less-right-to-be-forgotten-for-criminals-joran-spauwen-and-jens-van-den-brink/ (accessed on January 15, 2020)

- Burton, Graeme, France Orders Google to Apply EU 'Right to be Forgotten' Globally– or Face Action. COMPUTING, 12 June 2015, available at: http://www.computing.co.uk/ctg/news/2412884/france-orders-google-to-apply-euright-to-be-forgotten-globally-or-face-action (accessed on January 30, 2020)
- Otake, Tomoko, Right to be Forgotten' on the Internet Gains Traction in Japan, JAPAN TIMES, 9 December 2014), available at: http://www.japantimes.co.jp/news/2014/12/09/national/crime-legal/right-to-be-forgottenon-the-internet-gains-traction-in-japan/#.VkenSq6rRE5. (accessed on January 25, 2020)
- Concluding the EU Data Protection Reform Essential for the Digital Single Market, European Commission Fact Sheet, Data Protection Day 2015, 28 January 2015, available at: http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm (accessed on January 25, 2020)

- The Advisory Council to Google on the Right to be Forgotten, Advisory Council 2015, available at: www.google.com/advisorycouncil/. (accessed on January 30, 2020)
- Mayer-Schönberger, V. Omission of Search Results is Not a 'Right to be Forgotten' or the End of Google, The Guardian, 13 May 2014, available at: http://ejlt.org/article/view/75. (accessed on January 30, 2020)
- Commission Proposal for a Regulation of the European Parliament and of the Council, art. 4(2), 11 COM, 2012, 25 January 25 2012, available at: http://ec.europa.eu/justice/dataprotection/document/review2012/com_2012_11_en.pdf (accessed on December 7, 2019)
- Opinion 2/2017 on data processing at work, Article 29 Data Protection Working Party, WP 249, 8 June 2017, page 3 (accessed January 1, 2020)

LIST OF ABBREVIATIONS AND ACRONYMS

Art.	Article
CENDOJ	Centre of Judicial Documentation
CFR	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
DPA	Data Protection Authority
DPD	Data Protection Directive
DUI	Driving Under Influence
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EU	The European Union
FCRA	The Fair Credit Reporting Act
GDPR	General Data Protection Regulation
ICCPR	International Covenant on Civil and Political Rights
ICO	The Information Commissioner's Office
Para.	Paragraph/ s
RTBF	Right to be forgotten
SNS	Social Networking Services
TEU	Treaty on European Union
TFEU	The Treaty on the Functioning of the European Union

UDHR	The Universal Declaration of Human Rights
UK	The United Kingdom
US	The Unites States of America
WP29	Article 29 Working Party

CHAPTER 1: INTRODUCTION

1.1. Introduction

The English philosopher John Locke considered trust and prestige are the two elements that humans consider the most on the basis of which humans instinctually manage themselves with the purpose of leading the emersion of the self-concept.[1] Because of the Internet, the information is so willingly obtainable which remains online on a permanent basis, facilitates a permanent slandering on someone's reputation[2] which makes getting rid of from the past mistakes an implausible event since an indefinite amount of data can be achieved by inputting the data subject's name in a search engine.[3] Advanced information technological means, ever growing fast communication, cheap memory, easy retrieval, collection of personal data, archiving and above all strong recognition of right to freedom of expression took remembering capacity to an unimaginable level. The phenomenon of forgetting is anomaly nowadays since personal data is just one click away in Google search. Problem occurs when a particular information brings an adverse impact on someone's life by bringing facts to light. For example, in England, a woman's name was published as a criminal for murdering her husband which shattered her any chance to move forward with such a record since it became the fuel of numerous articles later on.[4] But now the existence of RTBF might provide some comfort to her plight[5] since EU citizens can request the search engines for removal of such information.[6] Facts might be parts of social media, news, archive or any other website directed through hyperlinks. The conflict of interest happens when someone is accessing, receiving or disseminating those facts while exercising his or her right to freedom of expression and other person of whom the information is concerned, trying to hide them for good which is the essence of right to be forgotten. Now, the big question is whether right to be forgotten can be considered as one of the restricting grounds of right to freedom of expression since both the rights have seen to

[1] King, Peter, The Life of John Locke: With Extracts from His Correspondence, Journals And Common-Place Books. Creative Media Partners, LLC, 2015, p. 109 (King 2015)
[2] Rustad, Michael L & Kulevska, Sanna, Reconceptualizing The Right To Be Forgotten To Enable Transatlantic Data Flow. 28 HARV. J.L. & TECH. 2015, pages 349, 353. (Rustad and Kulevska 2015)
[3] Ibid, page 352.
[4] Whitney, Lance, Google Hit by More than 144,000 'Right to be Forgotten' Requests, CNET.COM, October 10, 2014. (Whitney 2014) (accessed on January 8, 2020)
[5] Ibid
[6] Factsheet on the "Right to be Forgotten" Ruling (C-131/12), European Commission 2014. (Factsheet 2014) (accessed on January 15, 2020)

override each other. The phenomenon suggests that there is no standardized practice of establishing a definite norm.

From the enforcement of Lisbon Treaty, right to freedom of expression has become one of the fundamental rights in EU. Nonetheless, recent cases decided by the CJEU, along with ECtHR and other Union national courts have brought the question into light that what should be the scope of applicability of the right.[7] The formal inception of the right to be forgotten was introduced by the CJEU with the recognition of the Union citizens' having right to be forgotten.[8] And the right was enforced against the data processor Google, a legal person whose exercise of right to free expression was hindered. This is because in general, a successful exercise of right to erasure is performed through limiting the exercise of other's right of imparting or accessing or receiving the particular information which are essentially the elements of right to free expression. The CJEU confirmed in this regard that all those three abovementioned aspects relating to a data, constitutes the scope of the free expression right.[9] Thus, the highest court ruled against Google in favour of protecting personal information of the Union citizens through removing data from its search list which is detrimental to the fame. The idea is that search engine data controllers might *suo moto* wipe or they might be obliged to expunge certain information from the search list[10] when the data is represented with the identity of the data subject and here in this paper the data subject refers to the spent criminal convicts. However, the data can still remain in the original publishing website which is accessible directly from anywhere. Since protection of both the rights are related to protection of fundamental principles within the Union territory, the aiders of free expression tend to think that it is an ill founded impediment against right to freedom of expression.[11] But in reality, analysis of principles used in balancing approaches proved that there are no definite rules of determination, rather, at this point, elements of context specific determination need to be analysed.

There are so many people in the EU with a criminal record among which most of them are living as the law-abiding citizens of the society. The point is they already served their sentence

[7] Case C-101/01, 2003 E.C.R. I-12992, I-13004-06
[8] Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEDP), Mario Costeja González, Case C-131/12, 2014 ECLI:EU:C:2014:317, para. 100(3), May 13, 2014
[9] Case C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy, 2008 E.C.R. I-9831, para. 39, (May 8, 2008)
[10] Supra note 8.
[11] CFR, Art. 11, 2012 O.J. (C 326) 391, 398

and restored in the society through reformation. So, they do not have any connection from their past anymore. So, what happens when their criminal record details are online? According to Rosen (2012), it is the belief of the European lawmakers that an attempt from escaping anyone's past is almost impossible since the virtual world remembers everything and unlearn nothing and the phenomenon is far more aggressive for spent criminals.[12] Commissioner Reding (2010) rightly pointed out the particular risk for the teenagers who have entire life ahead and the risks of revealing lamentable information. She further added that if individuals do not want to keep a particular data online for further processing, then if there is not any lawful ground to keep it, it is the responsibility of the data controller to remove it from online.[13] However, she confirmed that it does not mean an entire erasure of the history.[14]

The 'google-effect' can be haunting for them for lots of different reason. Their past false step can cause public gaze over their existence, which might hinder their way to become the full and mass inhabitant and start a new beginning in a broader sense. For example, they face difficulty in securing an indispensable job, and related matters such as insurances, possessing a banking relationship, in some jurisdictions prohibition on travelling, or starting studying again which are certainly are not the meaningful felicities of courteous temporal community.[15] Nowadays, if a search is administered in the search engines with a name or any other identifiable term, unimaginable amount of collected data can be compiled so easily which are used to have an insight of a person. However, it is unlikely that all the information will be relevant to a particular individual, though it presents a lot. That is why even employers might choose to search somebody in the Google to have an idea about that person, in particular, what the Internet represents about him or her.[16] In fact, it became a constituent part of human common sense to 'Google' someone to find out enough information which could not be obtained otherwise. In that transaction, the available online news database plays a pivotal role in revealing past conviction records to anyone who performs search by putting in an

[12] Rosen, Jeffrey, The Privacy Paradox: Privacy and Its Conflicting Values. Symposium Issue, 64 STAN. L. REV. ONLINE 88, 13 February 2012, page 89.
[13] Viviane Reding, Vice President, Eur. Comm'n, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age 5, January 22, 2012).
[14] Reding, Viviane, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age, Innovation Conference Digital, Life, Design. Munich, 22 January 2012.
[15] http://www.unlock.org.uk/unlock-speak-at-ico-policy-conference-the-google-effect-criminal-records-and- the-right-to-be-forgotten/ (accessed on 3 May 2018)
[16] https://careers.workopolis.com/advice/the-three-things-that-employers-want-to-find-out-about-you-online/ (accessed on 5 May 2018)

unchangeable name.[17] This is unquestionably beyond the control of the data subjects. In this situation, of course, a distinct person's capacity to protect his or her e-reputation depends on how efficiently that person can control the emergence of personal information. The efficiency again depends on the context the information is accessed and what harm it causes exactly.[18]

Unfortunately, there are already so many instances which depict the negative impacts of 'google effect' where employers, insurers and other organizations used their criminal records and acted negatively that they should not be using. It is evident from the Article 29 working party opinion that there has been a trend of applying sophisticated means of data processing mechanisms at the overall work environment which implies to entire structure of functioning including applying for jobs and subsequently in the job place.[19] Article 88 of the GDPR fosters the conduction of employment process in a legitimate, transparent and proportionate way by imposing the obligations to the employers for respecting dignity, fundamental rights and lawful interests in employment related contexts. Because according to the Article 29 working party opinion, using publicly available information through social medias or any other sources available online is very common for employers to construct a personality image about a particular individual before recruiting.[20] However, this approach is not permitted by law unless the employer has a legitimate interest to do.[21] Unlike the United States, the EU legal system fosters ex-offender's privacy and reformatory rights.[22] So, the past affects the present and the future in a way which demands that individuals should be able to control exaggerated information about themselves so that no life remains permanent to an unchangeable future.

That is why after receiving a request of removing an information, the data controllers like Google, Yahoo and other third party processors should take into account the of such application with an assumption that the data subject's right to be forgotten would be respected on condition the sentence for the offence is over past.[23] However, an application will only be abdicated on the basis of any legitimate publication interests which is considered to outweigh the privacy

[17] https://christopherstacey.wordpress.com/2015/11/11/ the-google-effect-criminal-records-and-the-right-to-be-forgotten/ (accessed on 15 May 2018)
[18] Policy and Research Group of the Office of the Privacy Commissioner of Canada, Online Reputation, what are they saying about me? Discussion Paper, Office of the Privacy Commissioner of Canada, 2016, page 13
[19] Opinion 2/2017 on data processing at work, Article 29 Data Protection Working Party, WP 249, 8 June 2017, page 3 (accessed January 1, 2020)
[20] Ibid, page 11
[21] Ibid, page 14
[22] Jacobs, James B. and Larrauri, Elena, Are criminal convictions a public matter? The USA and Spain. Punishment and Society 14(1), 2012, pages 3-28
[23] Supra note 15

interests. But it does not elucidate a sound mechanism used by the data controllers whether to respect or reject a particular request of deletion. Though the GDPR vested great responsibility to the data controllers to comply with the legislation, it is not clear that if they have empowered themselves to set and follow a standardized mechanism since there are principles to respect right to be forgotten which need to be balanced with freedom of expression. For the interest of this paper, it needs to be equipoised in the case of criminal convicts who already past adjudication.

1.2. Objectives of the Study

This study tends to evaluate the research question and sub questions:

1. Is there a valid presumption that we guarantee Right to be Forgotten in Spent Criminal Convictions?

    1.1. What are the requirements of allowing right to be forgotten?
    1.2. How right to be forgotten and freedom of expression are balanced in spent criminal convictions in light of current case laws?
    1.3. How implementation of principles of right to be forgotten can be achieved in spent criminal convictions?
    1.4. How the analysis answers the main research question?

1.3. Limitations of the Study

The very basics relating to personal data protection for example: definition of personal data, difference between natural and artificial person and some others will not be covered due to having limited space. Besides, certain challenges of allowing right to be forgotten, for example, offshoots from historian viewpoint, extraterritorial applications of GDPR and related issues will not be covered. On the other hand, the discussion is limited to identifying the requirements of allowing right to be forgotten on the basis of case laws and Article 17 of the GDPR, balancing public and privacy rights mechanisms, identifying and applying right to be forgotten principles in spent convictions while arguments, structure and discussion will be narrowed down to analyze different characters of spent criminal convicts. Thus, it answered the final research question in the last chapter while confining the study within the EU legal framework.

1.4. Method

For the convenience of the study, doctrinal method has been chosen since the research has been designed to concentrate on the past felonious activities of the people who already served their sentences as well as the existing legal sources. Diversified cases will be studied and analyzed so that it helps not only to better understand different figures of the society but also how differently principles generated and applied in variant cases to determine the reciprocal weight each of the interests namely the publication and privacy carry and move towards a decision. The most prominent scholarly opinions in particular mostly writers on both the sides of privacy rights such as literatures from Victor Mayer-Scöhenberger, B. J. Koops, James B. Jacobs, Elena Larrauri, Corinna Coors, David Lindsay, Ugo Pagallo, Massimo Durante, Lawrence Siry, Kieron O'hara are the most remarkable that will be considered. As the study does not have any intention to outline any trend, quantitative apprehension lost its appeal for consideration. I believe, the approaches will uncover answers in thought and opinions and supplement the main research question by diving deeper into the problem.

CHAPTER 2: REQUIREMENTS OF ALLOWING RIGHT TO BE FORGOTTEN

2.1. Introduction

Right to be forgotten, an aspect derived from the privacy law of natural individuals, has the element of coercion which forces to forget a particular information from the Internet about a particular individual related to an event, that the person exercising right to be forgotten, wishes and becomes successful in exercising the right. Eventually, the lost information, if not censored, interferes with the right to information of the Internet users and if it becomes successful then, it invades users' free expression right. Keeping that in mind, RTBF is prescribed in GDPR with certain limitations. To put it differently, in order to exercise right to be forgotten, there are certain requirements that need to be satisfied. In this chapter, discussion is limited to the legal requirements of sanctioning right to be forgotten only while emphasis will be put towards the literal and pragmatic meaning of the right to be forgotten or right to erasure within.

2.2. Right to be Forgotten- Concept, Nature and Scope

The right to be erasure often referred as right to be forgotten became a legal right within the EU with the enforcement of the GDPR. However, whether it was a right or a value was controversial for a considerable period of time.[24] Some scholars perceived it as an ethical or social value,[25] and some other described as merit or objective policy.[26] However, Rouvroy's (2008) perception on the right is the most relevant for a better understanding of the true essence of the right. While finding the formulation of the right extremely interesting, Rouvroy argued that it should not be conceived as merely a legitimate interest to forget and to be forgotten.[27] In essence, it is related with individual centric development which entail anyone not to be stuck in anything what has been expressed, rather, everyone is always allowed to change and thus right to be forgotten strengthens the freedom of expressing oneself at large without the horror

[24] Koops, B. J., Forgetting footprints, shunning shadows. A critical analysis of the 'right to be forgotten' in big data practice. SCRIPTed, 2011, 8:1-28, page 231. (Koops 2011)
[25] Blanchette, J-F and Johnson, DG, Data Retention and the Panoptic Society: The Social benefits of Forgetfulness, 18 The Information Society, 2002, pages 33-45. (Blanchette and Johnson 2002)
See also, Dodge, M and Kitchin, R, Outlines of a World Coming into Existence: Pervasive Computing and the Ethics of Forgetting. 34 Environment and Planning B Planning and Design, 2007, pages 431-445.
[26] Mayer-Schöenberger, V, Delete: The virtue of forgetting in the digital age, Princeton: Princeton University Press, 2009. (Mayer-Schöenberger 2009)
[27] Rouvroy, A, Réinventer l'Art d'Oublier et de se Faire Oublier dans la Société de l'Information? Version augmentée, 2008, (self-translation), (Rouvroy 2008)

that the data might be detrimental for anyone in future.[28] Thus, Koops (2011) rightly said that a right to erasure often referred as right to be forgotten, is a legal right which is secured through the operation of law or any other legal mechanisms. Reding's (2012) claimed that a RTBF would clarify and make other rights strong since a RTBF would empower the data subject to have a data removed if it is proved that the data is retained for longer period than necessary, or an objection against unauthorize use of a piece of data is justified. On the basis of Redding's claim, Koops (2011) identified data in the way of memories in two folds: failure of accessibility and failure of availability in the Internet.[29] To make the distinction clear, he argued

- a RTBF occurs after following a due process and time lapse is an important factor
- a RTBF is essentially a right to 'clean slate' which bars in using a particular data against the data subject after certain period of time and
- a RTBF guarantees a right to freedom of expression in a way which eliminates the risk of using the voice or processing which otherwise would have used against the data subject.

So, the first point is connected with diminishing the availability of the memory while the last two points are concerned with carving accessibility to the concerned memory.

The right is demanded when it concerns the need to be forgotten by the third parties about the data subject's past memories. In essence, the idea of RTBF lies within passive implication to manifest forgetfulness. It needs to be remembered that right to forget and right to be forgotten are different concepts in themselves. The first one involves active form of occurrence, but the later form is passive. It is true that it is important for the first person, the data subject to be capable of forgetting his or her own past. For this reason, the passive force to be forgotten which is applied to others emerged in the name of right to be forgotten so that others do not contradict with the data subject's active right to forget. That is why though forgetting is the intrinsically natural operation of human brains the idea of right to be forgotten does not refer to psychological function, rather a need which demand legal reinforcement as such.[30] However, the idea itself does not involve erasing something artificially from someone's memory, rather removing or hiding something from the Internet so that it becomes difficult for others to find

[28] Ibid, pages 25-26.
[29] Koops, Bert-Jaap, Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to be Forgotten' in Big Data Practice. Social Science Research Network, December 20, 2011. (Koops 2011)
[30] Parker, ES. Cahill, Larry and McGaugh, James L., A Case of Unusual Autobiographical Remembering, 12 Neurocase, 2006, pages 35-49. (Parker 2006)

and publish the embarrassing information further since now this a era of Web 2.0 which empowers users to create data by themselves which can essentially be data about others with and without other's permission.[31] So, there is a collective effort for remembering a particular event about someone which completely independent in nature and beyond control of the data subject because there might be multiple memorizers of an event.

The issue in particular, the way how certain event has been perceived and memorized by the witnesses or the people around the data subject. The problem sparks concerns while in the future, the event or data confronts the data subject in a way which is contradictory with the horizon of expectations of the data subject and of the society about the data subject which paves a broader leeway against the data subject to have negative repercussions which affects his or her personal life and privacy interests robustly. For example, if Mr. A cuts up something before Mr. B and Mr. C against the norms of his society, after sometime it has been found that Mr. B forgot about what happened, but Mr. C did not, rather, Mr. C reminds Mr. C reminds Mr. B of the happening. So, the collection of all the memories is undoubtedly plump which might involve difficulty in hiding. In this regard the folk cognition can be illustrated which says individuals have to subsist with all the consequences.[32] The mind-blowing tale of Abu Hassan is worth sharing in this context which is narrated in the book of 'One Thousand and One Nights' and tale itself titled 'The Historic Fart'. The legendary tale evolves with the introduction of Abu Hassan's thundery fart in his own weeding day which is believed to be echoed which made all the guests fully silent. After this faux pas, he left his living place for being ashamed and embarrassed for ten consecutive years. His homesickness brought him back to with the perception that people might have forgotten everything within this long period of time. Pouring cold water on his hope, he found that he is not forgotten, rather he along with his faux pas committed ten years ago became a temporal standard within the society. For instance, upon a child's asking to his mother about the time of his being born, her mom replied that it was at least ten years since the same year Abu Hassan farted. This forced Abu Hassan to disappear from his community for good.[33]

[31] The Digital Universe Decade (2010) available at http://www.emc.com/collateral/demos/microsites/idc-digital-universe/iview.htm (accessed 1 Nov 2011)
[32] O'hara, Kieron, Shadbolt, Nigel and Hall, Wendy, A Pragmatic Approach to the Right to Be Forgotten, Global Commission on Internet Governance, Paper Series No. 26, March 2016. (O'hara, Shadbolt and Hall 2016)
[33] Ibid

The plot of the story urges the need of having some mechanism in the hands of Abu Hassan so that he could try to conceal the memories which used to baffle him since the later chapters of the story construed upon the perception and interpretation of the collective memories on how people represent those irrespective of accuracy or inaccuracy on which Abu Hassan had no control over.[34] Unfortunately, he did not have any way to adhere to so that he could seek for forgiveness unlike the present day.

From data processing point of view, Gross and McIlveen (1999) believed that there are three steps which makes up a memory: 1. registering a data in a storable form, 2. storing the data permanently by using memory retention hardware and 3. salvation of the data from retained storage.[35] Here, the concerned data has essentially been registered already which is contained in a storage. So, there still remains two crucial and most relevant thoughts regarding RTBF: the data is not available anymore meaning data is not stored anymore, and the data is not accessible anymore which means though the data is stored, it cannot be retrieved so easily. In order to remove the entire data from the Internet, all the links have to be deleted. On the other hand, if very few selected links are erased, then it makes the retrieval difficult, not impossible.[36] The later concept has been accepted for interpreting the meaning of RTBF by Union authorities which will be discussed broadly later on.

Undoubtedly, the right to be forgotten is an intellectual outcome of the European legal system. In particular, the idea had been found in French legal system which was known as *le droit à l'oubli* which means right of oblivion which was directly linked with the spent criminal convicts who wanted to lead their lives as reformed and rehabilitated citizens.[37] The primary objective was to prevent the publication of the facts related to their convictions and confinements. It appears to be such information which has been recorded by third parties such as the court, journalists and other sources. However, it triggers other related questions to understand the true meaning and scope of the application of right to be forgotten such as, does the right applies to the situations where the information in question is circulated by the data subject oneself? Even if the data subject publishes, what would be the case if the data has been

[34] Ibid
[35] Gross, RD. Richard and McIlveen, R. Memory, London: Hodder & Stoughton, 1999. (Gross, Richard and McIlveen 1999)
[36] Supra note 32.
[37] Supra note 35, see also, Commission Proposal for a Regulation of the European Parliament and of the Council, art. 4(2), 11 COM, 2012, 25 January 25 2012. (accessed on December 7, 2019)

copied by others and circulated further? Apparently, the law defined broadly already which is to state, 'any information related to a data subject'.[38] To understand these scenarios as well as the scope of RTBF, Google's contemporary chief privacy counsel Peter Fleischer's (2011) concerns would be evaluated here which he had written in his blog[39] to see the levels of controversies to have a deeper insight of the scope of right to be forgotten.

In his blog post, he expressed his concerns in three different scenarios. Firstly, in case, somebody posts his or her own information online through different forums such as social media platforms such as Facebook or Twitter. But later on, the data subject decides to remove it from the concerned platforms. What might be the case in this situation? Well, the situation appears to be already under control since the social media websites already have put forward the mechanisms of deleting or removing the contents from their platforms by users on their own. Besides, according to the privacy policy, if they commit to delete or remove the content from their data bank, the authority can force the controllers to do so. In this case, the exercise of the right is self-initiated and in offensive.

In the second situation, the level of controversy is much higher. The situation is perceived as the data subject disseminates the information in question *prima facie,* but third parties viz, friends and families continue to re post or processing by other means afterwards. Does the subject have a right to have the data removed which is being processed by friends, family members in a social media platform or even removed from any of the lists of search engines? The answer is unlikely simple as the first one. It appears that the data subject can ask the controller in this case the social media platform and even the search engine operators to remove it since Art. 17(1) of GDPR binds the controller to remove the content without any delay unless it is justified on the ground of freedom of expression under Art 17(3) of the Regulation. However, there are still exemption since Art. 80 provides further exemptions on the right which allows to continue the processing on the grounds of the processing's being for the purposes that serve journalistic, artistic or literal expression interests. However, since the responsibility is upon data controllers, in order to continue the processing, the social media platforms need to prove that processing is continuing on the basis of any of the lawful grounds. However, if it appears to the data controllers after taking reasonable steps that it should be taken down, the

[38] *Ibid*
[39] Fleischer, Peter, Foggy Thinking About the Right to Oblivion. 9 March 2011. (Fleischer 2011) available at: http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html (accessed on January 7, 2020)

controller can do so and *vice versa*. So, even in this situation the complexity is greater than the previous scenario and the data subjects might still some control in posting or sharing information of their own.

The last and the most complicated scenario is that if a third party by its own initiative publishes something about the data subject which is true but defamatory, does the data subject has the right to remove it? This is purely a question of exercising freedom of expression. Focusing on two provisions: first, the definition of personal data contains the phrase 'any information relating…'[40] which draws attraction of data protection laws, second, freedom of expression is not absolute under Art. 10(2) of the ECHR, it can be said easily that at least the data subject has the right to seek removal of the data. In this situation, it is again the data controllers, or DPA or the local courts who have to decide the future of the processing at stake. If it legitimately falls within the scope of processing on the basis of journalistic, artistic or literary interest, then the data subject might face a rejection against a removal request. However, in this situation the determination of RTBF does not depend merely on these grounds only. There are some other factors too which is developed after the Regulation came into force. To make this clear, while being ambitious, Commissioner Reding stated that the Regulation has been framed to stand for 30 years and so it has to provide shelter for new future technologies which can be done through roofing the changes of the market and public opinions.[41]

This paper deals with the last and the most complex scenario of right to be forgotten in which the spent convicts are the data subjects and their personal related to their convictions and incarcerations have been made available online by the third-party initiatives such as judgments, news, social medias, blogs and others.

According to Margalit (2002), right to be forgotten inherently contains the substance of forgiveness and the forgiveness essentially means the debt that has been generated by the data subject previously by one's faux pas or wrongdoing[42], the debt has been paid while the criminal must march forward in life so that he or she can repossess the mastery through the passage of time and find him or her in the everyday society again (Augé 2004, 88).[43] The RTBF has been

[40] Article 4(1), GDPR
[41] Warman, Matt, EU Fights 'Fierce Lobbying' to Devise Data Privacy Law. TELEGRAPH (Feb. 9, 2012). (Warman 2012)
available at: http://www.telegraph.co.uk/technology/internet/9069933/EU-fights-fierce-lobbying-todevise-data-privacy-law.html. (accessed on January 5, 2020)
[42] Margalit, Avishai, The Ethics of Memory, Cambridge, MA: Harvard University Press, 2002. (Margalit 2002)
[43] Augé, Marc, Oblivion, Minneapolis: University of Minnesota Press, 2004. (Augé 2004)

introduced to award data subjects to exercise the right in a defined form due to utilitarian reasons which are related to the rehabilitation of the offenders through restricting the access to their conviction data. The UK law on Rehabilitation of Offenders Act 1974 permits the spent convicts to conceal their past criminal data in specific circumstances such as when applying for jobs, performing any civil action though it depends on the graveness of the crime. In addition, in Germany, criminal's name is usually withheld while reporting any news on condition that the sentence has been served already. Siry and Schmitz (2012) stated that the German court outlined the empowerment of the spent convicts to reintegrate with the society as one of the grounds of their privacy rights.[44] On the other hand, publication interests of the journalists, right to access of the historians and reporting rights publicly as some of the grounds of respecting freedom of expression. This is one direction of justifying RTBF. It needs to be mentioned that the number of permanent criminal record holders are very high in number nowadays.[45] For example, according to BBC (2015), a 14 years of age citizen of the UK discovered himself in the national media coverage for committing a crime which was disseminating inappropriate pictures of a child. Apparently, the picture in question was of his own naked one which he sent via message service to a girl who shared the photo with others. Consequently, his misdeed was registered into the law enforcement agency's database as a crime which might pose a disproportionate negative effect in his later life in particular, if he wants to get involved with children activities.[46]

It is to be mentioned that Union Members maintain National Conviction Register (NCR) to have records of criminal convictions. However, communications with enforcement bodies are not a constituent element of criminal conviction records though the situation is slightly different in England and Wales where even warnings and blusters related to offences are also recorded along with criminal conviction information.[47] Nowadays criminal cases are also disposed in particular Member States without direct adherence to the traditional conviction procedures. For

[44] Siry, Lawrence and Schmitz, Sandra, A Right to be Forgotten? How Recent Developments in Germany May Affect the Internet Publishers in the US. European Journal of Law and Technology 3 (1), 2012. (Siry and Schimitz 2012)

[45] Supra note 26.

[46] "Sexting Boy's Naked Selfie Recorded As Crime By Police." BBC News, September 3, 2015. (BBC 2015) (accessed on January 3, 2020)

[47] Jacobs, James B. and Larrauri, Elena, European Criminal Records & Ex-Offender Employment, University Public Law and Legal Theory Working Papers 532, New York: Oxford University Press, 2015, page 3. (Jacobs and Larrauri 2015)
See also, Larrauri, Elena, Are police records criminal records? Disclosure of criminal information and the presumption of innocence. European Journal of Crime, Criminal Law and Criminal Justice 22, 2014, pages 377-395, (Larrauri 2014)

example, the mechanism is available in the Netherlands where the term 'transaction' is used instead of prosecution in which an agreement is executed between the complainant and the defendant where defendant might be obliged to pay a fine or carrying out other social services which are also considered as criminal convictions and not shared generally.[48]

In the foregoing sections and chapters, requirements of allowing right to be forgotten of the spent convicts as well as the balancing adherences, and the fundamental principles regulating the norms will be outlined.

2.3. Requirements of Right to Be Forgotten

Before GDPR came into force in 2018, the European Data Protection Directive of 1995[49] existed which is repealed with the enforcement of the GDPR. Unlike the GDPR, the Directive of 1995 required the Union Members to enact laws to protect individual personal data from unfair and unlawful processing.[50]

Meanwhile, the courts and tribunals in the Member States were seen to be considerably active to deal with the RTBF issues, in particular, the French '*Tibunal de grande instance de Paris'*, Italian '*Corte di Cassazione'*, and Spanish '*Audencia Nacional in Madrid'*.[51] Firstly, in February 2012, *Tibunal de grande instance de Paris* ordered Google to erase all the links that identified the applicant Diana Z. to her previous activities related to porno performances from its .com and .fr domains. The decision raised controversies due to the safe harbor clause of immunity for the Internet Service Providers under Art. 15 of the e-commerce Directive (D-2000/31/EC). Then it went beyond the search engines in April 2012 when the Italian *Court of Cassation* based in Rome directed that Internet archives also should maintain the accuracy of an information through upgradation so that RTBF requests can be enforced. On March 2012, the Spanish court was already dealing with the analogous situation in its case C-131/ 12 in which the *Audencia Nacional* submitted the matter for preliminary ruling to the CJEU seeking

[48] Ibid
[49] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L 281/31)
[50] Ibid, 10.
[51] Pagallo, Ugo and Durante, Massimo, Legal Memories and the Right to Be Forgotten, Protection of Information and the Right to Privacy- A New Equilibrium?, Law, Governance and Technology Series 17, Springer International Publishing Switzerland 2014. (Pagallo and Durante 2014)

particular directions towards individual's entitlement of seeking remedy under RTBF[52] which later on became the first and most important judgment adhered into by the highest court of the Union in the area of RTBF, known as *Google Spain* ruling.

After *Google Spain*, multiple government authorities such as radical DPAs, Article 29 Working Party, and national courts tended to develop RTBF. Firstly, the Working Party proved to be the most efficient institution outlining RTBF guidelines in 2014. After performing extensive consultation with Google, the Party published a set of thirteen criteria for considering a RTBF request which is applicable for the search engines.[53] Secondly, the DPAs also retain the power to impose their decisions on search engines like Google by reviewing the decisions disposed by the search engines on condition that the claimant appeals.[54] There are few examples in which the DPAs had their decisions, for example, French DPA ordered Google to remove all claimant's links from all of its domains worldwide though that has been appealed later on.[55] Lastly, since the data subject can appeal to the national courts against any decision of a DPA, national courts also a role player in developing RTBF. In 2012, the Amsterdam court backed up Google's decision of not allowing right to be forgotten in which the matter was to remove a criminal record article of an individual who used to run an escort providing services and was found guilty for 'attempted incitement of contract killing' which took place in 2012.[56] The court further stressed on the CJEU findings in *Google Spain* ruling and stated that a RTBF does not protect the data subject from any form of discrepant processing, rather, only protects from 'being pursued' 'irrelevantly, excessively or unnecessarily'.[57] However, other courts are free to apprehend towards more comprehensive approaches in outlining requirements and for providing guideline relating to the scope of RTBF if necessary, refer matters to the CJEU.

The CJEU already confirmed that personal data protection right is a primary right for every natural individual which is confirmed by Art. 8(1) of the CFR, 16(1) of the TFEU.[58] In addition,

[52] Ibid
[53] Art. 29 Data Protection WP, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González C-131-12, at 3, 9, 14/EN WP 225, November 26, 2014.
[54] Lee, Edward, Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten, 49 U.C. Davis L. Rev. 1017, 2016, page 31. (Lee 2016)
[55] Schechner, Sam, French Privacy Watchdog Orders Google to Expand 'Right to Be Forgotten,' WALL ST. J. 12 June 2015. (Schechner 2015)
[56] Spauwen, Joran & Brink, Jens van den, Dutch Google Spain Ruling: More Freedom of Speech, Less Right to Be Forgotten for Criminals. Inforrm's Blog, 27 September 2014. (Spauwen and Brink 2014)
[57] Ibid
[58] Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), C-507/17, 24 September 2019, paragraph 46.

the right is conditional and must be interpreted and enforced in a symmetric way with other dominions of the same status in which proportionality principle would have to be taken into account.[59]

Furthermore, the Universal Declaration of Human Rights (UDHR) forbids to be subjected as any unrestricted thrusting against someone's privacy rights. Article 12 of the UDHR, stated

> "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[60]

Before shading lights on statutory requirements of RTBF, little apprehension towards accessing into information aspect of right to freedom of expression is plausible since the opponents of right to be forgotten see the right as a threat against right to freedom of expression. For example, according to Jeffrey Rosen (2012), the outcome of right to be forgotten through GDPR is not a delicate expansion of a privacy right, rather, it is one of the largest denunciations against freedom of expression online.[61] The court opined that the serious crime will be relevant in order to be able to qualify a RTBF claim, it has to be excessive and unnecessarily defamatory. In particular, if the offence records are brought up to light without any transparent reason, in particular, in no purpose but to damage the reputation of the data subject involved.[62]

2.3.1. Propagation towards free expression right in particular right to access to information

Right to freedom of expression is dealt by both Article 10 of ECHR and Article 11 of CFR. All EU Members' being signatories to ECHR, it is applied in the EU. Besides, with the enforcement of Lisbon treaty in 2009, the CFR also came into force in the EU. Consequently, even the CJEU seeks these two instruments while ruling.

Article 10(1) of ECHR and Article 11(1) of CFR denote a very broad scope of this right in three folds: holding opinion, imparting information and receiving ideas and information. In addition to that Article 19(2) of the ICCPR, also define right to freedom of expression almost

[59] Ibid, page 4.
[60] Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948).
[61] Supra note 12.
[62] Supra note 56.

identically.[63] Supporting the law, the CJEU opined, the scope of freedom of expression is not limited to its literal meaning which is to express the thoughts only, rather, it extends till all the derivates of taking in and conveying facts.[64] Again, in 2009, the CJEU broadened the scope of taking in facts[65] through a ruling of this particular case. The same approach has been reaffirmed in another case[66] where the honorable Justice acknowledged that a right to taking in information is essentially an aspect of entering into that information. Furthermore, while reassuring again, the court reminded again that the liberty of receiving data comprise of ingression of data.[67] So, the norm of the right is well established within the framework of Union law,[68] though subsequent sub Article 10(2) of ECHR 19(3)(a) of ICCPR mention certain limitations of exercising this right making it a non-exclusive right among which restriction is justified for the protection of the rights of others.[69] Undoubtedly, the law itself does not envisage the absoluteness of this right. So, there ought to be a balance between exercising one's right to freedom of expression and rights of others.[70]

2.3.2. Requirements of right to be forgotten or right to erasure

It is inevitable to look into the requirements of allowing a RTBF since without apprehending towards the requirements, it is impossible to strengthen and set out detailed data protection processes, obligations and enforcements. The CJEU rightly affirmed that for meaningful protection of personal data throughout the Union demands to define the entitlements of the data subjects through rights and protect those through bringing charges against the controllers of individual data for any of the violations of those rights. It further added the necessity of detailed outlining of monitoring and punishment mechanism to ensure a better compliance with the rules.[71] However, this discussion is limited to outlining the rights and principles of the RTBF.

2.3.2.1. Requirements under case laws with special reference to Google Spain case

[63] Oster, Jan, Media Freedom as a Fundamental Right. Cambridge University Press, June 2015, pages 69 and 147. (Oster 2015)
[64] Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy, Case C-73/07, 2008 E.C.R. I-9831, para. 39.
[65] Társaság a Szabadságjogokért v. Hungary, 37374/ 05, 14 April 2009, paragraph 35.
[66] Österreichische Vereinigung zur Erhaltung, Stärkung und Schaffung v. Austria, 39534/07, 28 November 2013, paragraph 41.
[67] Youth Initiative for Human Rights v. Serbia, 48135/06, 25 June 2013.
[68] Maduro, Miguel Pojares, Interpreting European Law: Judicial Adjudication in a Context of Constitutional Pluralism. 1 EUR. J. LEGAL STUD. 2007, pages 138, 146. (Maduro 2007)
[69] Supra note 63, page 147.
[70] Article 10(2), ECHR
[71] Supra note 58, paragraph 11.

Sometimes it has been seen that petty criminal cases had huge impact on perpetrator's private life due to the presence of the embarrassment element, such as accusation for urinating in an open public place where urinating is not allowed. The problem is really huge when it appears as the top search result or even in the first page of the search list. But what happens if the newspaper archive fails to put the full story or even the search engine does not show the news of the same person's acquittal in the same page? However, it needs to keep in mind that though the first news of bringing charge against the data subject is true so as the acquittal. But since the users are mostly interested only to look into the first page, it is possible that the information might mislead them to create a mental summary or misrepresent the data subject. The *Google Spain* case has more or less the same gist in which the primary cause of action arose with the digitization of the version of concerned newspaper. To put it differently, the online news archive of the newspaper.

Ruling of this groundbreaking case came in 2014 from the highest court of the Union jurisdiction. The facts of the involves that Mario Costeja González, the claimant sued particularly against two newspaper pages which contained data relating to the claimant's outdated past. Considering the publication year, which was 1998, the online archival of those data was claimed to be irrelevant and inaccurate. To be more specific. the complaint was on the basis of irrelevancy with his reputation and impertinency to public interest since the matter was decided more than a decade ago.[72] They represented an incomplete part of the claimant's life story by publishing only the event of the coerced sale of his owned housing property due to having a loan, but the retaking of the same after reimbursing the same loan was not posted in any relevant posts or anywhere. The case is mostly known as the *Google Spain* "Right to be Forgotten" ruling, where the man complained that Google's search results of his life event infringed his privacy. The case is a landmark for both: recognizing right to be forgotten and this paper which discusses right to be forgotten in spent criminal convictions. In this case, the right to be forgotten is established for the applicant who at the first instance, failed to comply with legal requirements of paying debt, but later on, became successful to secure the ownership his house lawfully after paying the debts. The court found the request in his favour and recognized a RTBF for the first time.[73] So, formal recognition itself is derived from an adjudication which helped the applicant to remove those records which concerned his lawfully paid off debts but was still available online. Certain principles were brought to light through

[72] Supra note 8, at 317 § 1and § 14.
[73] Ibid, page 3, paragraph 2.

this judgment which made the requirements of allowing RTBF evident. The requirements formulated by the *Google Spain*[74] on the basis of Articles 7 and 8 of the CFR, Art. 8 of the ECHR and Directive 95/46/EC:

- In defining RTBF and its scope: the RTBF is exercised when a search engine operator erases the links (delists or deindexes) published by third parties which contain certain information about the individual, from its list of results when any search is initiated on the basis of that individual's name,[75]
- In applying RTBF: if the tidings of the information deem to be 'inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue' made by the data controllers,[76]
- In determining *locus standi*: the claimant has been exempted from showing any prejudice caused by the information,
- In balancing against other rights: in the condition of the information's being 'inadequate, irrelevant, or no longer relevant, or excessive in relation to the purposes' of the processing, the court conditionally prioritized RTBF over financial interests of the search engines and the interest of the public,
- In outlining rebuts: at the time of prioritizing RTBF, nature and sensitivity of the information in both to the person's private life and public interest can be taken into account to rebut against allowing RTBF.[77] In this situation, whether the person is involved in any public role or figure, might be taken into consideration. In addition, the right is not exclusive in nature, but a proper balance needs to be struck against other primary rights, viz, right to freedom of expression or of the press[78],
- In mentioning duties and responsibilities: in determining each case, the search operators under the definition of data controllers are vested with the responsibility to move towards context specific determination (case-by-case) only[79],
- In describing appealing procedure: in case the RTBF application is rejected or refused, the applicant is allowed to go to privacy authorities or courts of law to challenge the

[74] Ibid, see also, supra note 53, paragraphs 7-10.
[75] Ibid, paragraph 94.
[76] Supra note 74.
[77] Ibid
[78] Supra Note 6
[79] The terms "data subject" refers to an identified or identifiable person about which specific data relates. Art. 4(1), supra note 40.

decision. However, the data controller is not in position to appeal any decision if RTBF is allowed.[80]

In *Google-Spain*, the honorable court outlined a series of coherent requirements which needs to be fulfilled in order to be able to establish a claim of RTBF. The court found its motivation to limit the application of right to be forgotten in the language of right to de-referencing or de-indexing to the search engine operators like Google and others while keeping the information as it remains to the publishing site which the court termed 'third party' which hosts the data at bottom.[81]

In terms of tangible requirements, the court identified firstly, if the de-indexing request information appears on the basis of an identical name and displays in listing orientation, irrespective of the algorithmic priorities of the search engine operators. Secondly, the court attracted RTBF upon the attainment of the objective of the questioned data for which it was collected or processed at the first instance.[82] Thirdly, the data has to be removed if found inadequate, irrelevant or no longer relevant, or excessive in connection with the processing purposes of the data controllers at all circumstances.[83] Last but not the least, the impact of the data in data subject's private and family life also has be taken into account.

In terms of enforcement of the right, the court ruled that the de-listing must be effective when any search is sought in any particular name and the information which has been respected with right to be forgotten, is not available for common people anymore in the way of listing or charting in any search result.

In this situation, the privacy rights under Art. 7 and 8 of the CFR, Art. 8 of ECHR and Art. 17 of GDPR trample the legitimate business interests of the search engines and legitimate interest of the public in that particular information. The language derives the limitations of right to be forgotten referred by the court which are legitimate business interests of search engine operators and interest of the public.

[80] Burton, Graeme, France Orders Google to Apply EU 'Right to be Forgotten' Globally– or Face Action. COMPUTING, 12 June 2015. (Burton 2015)
[81] Supra note 6
[82] Supra note 8, judgment summary, page 2, paragraph 6.
[83] Ibid

However, the *Google Spain* ruling would not be the same if the claimant or applicant Mario Costeja González had any public role or the common people had any legitimate interest in his activities for his being a public figure or public activities. In that case, the interference in his public life would have been justified by publics' interest and thus, he would fail to fulfill the requirements of allowing right to be forgotten. The concept of public interest will be discussed in chapter four.

In short, though the Directive 95/46/EC did not guarantee RTBF explicitly, the court interpreted the relevant provisions of the law in the *Google Spain* judgment in a way which facilitates data subject's claim to exercise RTBF while the court relied not only on data subject's right to access to its own data but also in the event of not comporting with the Directive provisions, entitled the data subject to ask for correction, efface, interruption or even objection against those, which is the exact reflection of GDPR jurisprudence which repealed the Directive and will not be excessive if it is said that GDPR contains more comprehensive provision today comparing with the original case law, derived from *Google Spain.*

In stressing the significance of Art. 17 of the GDPR, the CJEU confirmed in a case[84] that the data subject's right to de-referencing found its base on that respective Article which in particular governs the matter of right to be forgotten or right to erasure.

2.3.2.2. Requirements under GDPR

Different Recitals and Articles of the GDPR deal with personal data protection regulatory matters when it comes to the spent criminal convicts which depict not only the objectives and purposes of the law but also the tangible requirements in a clearer and broader context. After analyzing the requirements, it is found that those are coherently intertwined version of Recitals, Articles and Principles of GDPR.

Natural person's protection (here the data subjects are the spent criminal convicts) from the processing of their private datum has been perceived as an elemental right in Recital 1 with special reference to Art. 8(1) of the Charter of Fundamental Rights (CFR) and Art. 16(1) of the TFEU. While respecting all other fundamental rights mentioned in other Union documents, Recital 4 mentions the non-exclusive nature of data protection right which can be supported by one of the fundamental principles of the EU law, the principle of proportionality under Art. 5

[84] Supra note 58, paragraph 46.

of the TEU. Besides, the necessity of protecting sensitive data which has been understood as creating threats to fundamental rights and freedoms, attracts special protection merit[85] though derogation is also possible on grounds of protecting personal data and other primary rights[86]. Last but not the least, though Recital 19 vests regulation responsibilities upon Member States for processing personal data related to criminal convictions and offences matters which are processed by the public authorities, Recital 65 addressed a data subject's right to be forgotten directly to be obtained of course upon establishing a breach of this Regulation provision from the respective data controller subject to the Union jurisdiction.

The right is enshrined directly in Article 17 of GDPR. The right to be 'forgotten', known as the right to erasure, gives individuals not only the ability to request the removal of their personal data within justified time when no compelling justification is put forward by the data controllers (companies who fix the purpose of processing the concerned data at a specific time), but also makes the data controllers liable to remove the concerned data within reasonable time on the basis of one of the subsequent grounds apply namely, the data fulfills the collection or processed purposes[87], data subject's being revoking the consent for processing[88], the data subject exercises right to object under Art. 21[89], the data being processed illegally[90], in compliance with any legal obedience under Union jurisdiction[91], and data being collected in serving any Information Society service to a child under 16 years of age without the consent of the parental authority[92].

However, to discuss the derogations under Article 17(3) of the GDPR, a right to be forgotten can be restricted on any of the following grounds: exercising right to freedom of expression[93], or performance of task carried out in public interest or delegated official mastery[94], or public interest matters in scope of public health[95], or for record room reasons in the 'public interest, scientific, or historical research, or statistical purposes[96] or establishment, and exercise or

[85] Recital 51, General Data Protection Regulation, Regulation (EU) 2016/679.
[86] Recital 52, Ibid
[87] Article 17(1)(a), Ibid
[88] Article 17(1)(b), Ibid
[89] Article 17(1)(c), Ibid
[90] Article 17(1)(d), Ibid
[91] Article 17(1)(e), Ibid
[92] Article 17(1)(f), Ibid
[93] Article 17(3)(a), Ibid
[94] Article 17(3)(b), Ibid
[95] Article 17(3)(c), Ibid
[96] Article 17(3)(d), Ibid

defence of legal claims'[97]. These are those possible compelling justifications, any of which can override someone's right to be forgotten. So, like right to freedom of expression, the right to be forgotten is also not exclusive, needs to be weighed against other dominions before applying.[98]

So, Art. 17(1) prescribes the exclusive grounds on the basis of which right to be forgotten can be respected. On the contrary, Art. 17(3) puts certain limitations for deterring practice of right to be forgotten. These abridgements are outlined as the intertwined version of data processing principles and lawfulness of processing under Article 5 and 6 of the GDPR respectively. That is because the notion of unlawful processing of data hinges with Article 6 directly which details the grounds of lawful processing. To put it differently, any processing which does not comply with any of the grounds Art. 6 can be classified as unlawful processing, and Article 17(3) clarifies the derogatory justified grounds on the basis of which unlawful processing can be allowed. However, deeper discussion on lawful and unlawful processing is inevitable as one of the balancing principles in chapter four.

2.4. Conclusion

Analyzing the requirements of the right to be forgotten, it is perceived that application for exercising RTBF can be made in multiple situations. However, the law itself inflicts limitations on laying out the right among which wielding right to freedom of expression is one of the grounds of disapproving. Since this public right is also not exclusive and subject to certain limitations, it needs to be balanced on the basis of established principles of law. The next chapter tries to identify balancing issues, as well as finding the gaps in balancing. In doing so, it tends to discuss and analyze the existing principles so that the missing principles of balancing in spent criminal convicts can be identified in comport with GDPR.

[97] Article 17(3)(e), Ibid
[98] Concluding the EU Data Protection Reform Essential for the Digital Single Market, European Commission Fact Sheet, Data Protection Day 2015, 28 January 2015, available at: http://europa.eu/rapid/press-release_MEMO-15-3802_en.htm (accessed on January 25, 2020)

CHAPTER 3: BALANCING RIGHT TO BE FORGOTTEN WITH FREEDOM OF EXPRESSION IN SPENT CRIMINAL CONVICTIONS SO FAR

3.1. Introduction

From the origin of right to be forgotten, one of the derivatives of privacy rights, the primary issue which has been seen is the balancing efforts between this privacy right and other public rights since the primary right for personal data protection is not an unconditional right, rather, its societal function also has to be taken into account according to the norms of principle of proportionality and Union common interest to meet its objectives to protect others' rights and freedoms[99]. After getting recognition from GDPR, the right to be forgotten found its strong base, in which public right to freedom of expression has been prescribed as one of the reasons of limiting right to be forgotten. So, balancing is inevitable. Even the ECtHR and CJEU stressed multiple times that when applying privacy rights under Art. 8 of ECHR and Art. 8 of CFR, a balanced proceeding with other rights is indispensable.[100] The balancing mechanisms between privacy and public rights, most relevantly, between right to be forgotten and right to freedom of expression gave birth to those relevant balancing principles, which are responsible while determining whether right to be forgotten would be allowed or not. In this regard, understanding the gradual development of conflicting issues between these two rights is extremely important to understand the balancing points derived from different viewpoints of Union law.

3.2. Persistent Issues Derived from *Google Spain*

The points derived of *Google Spain* ruling is one of the focal points as it is the first recognition of right to be forgotten of EU citizens which depicts the first generation of right to be forgotten as well as the balancing initiative between right to free expression right and RTBF.

[99] Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, C-92/09 and C-93/09, 9 November 2010, para. 48.
[100] Productores de Música de Espana (Promusicae) v. Telefónica de Espana SAU, C-275/06, 29 January 2008, para. 68. See also Council of Europe (2013), Case law of the European Court of Human Rights concerning the protection of personal data, available at: www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP 2013 Case Law_Eng_FINAL.pdf.

3.2.1. Tension in balancing between public access to information and privacy rights

While ruling the RTBF case, the honorable court used such languages which is responsible to incite the controversy between penetrating into information and right to protect private data.[101] The CJEU exactly meant that since a RTBF is not an exclusive right, it will seize to subsist unless it has been balanced with other similar dominion such as right to free expression or other publication rights.[102] To put it differently, precedence of right depends on each context. In many cases, the CJEU considered it to be justified to allow access at will to information,[103] especially true under Art. 85(1) when the data is not used unlawfully and under journalistic purposes exemption.[104]

The spent conviction information in the form of 'personal data'[105] remains in the web and who is to determine whether the data subject has the RTBF or not. Because while assessing 'public interest' as one of the overriding justifications of RTBF, the honorable court held that in cases where a 'legitimate right to removal'[106] is found, that right overrides public's interest in finding that particular information on the basis of that person's name. It further said, acceptance of an individual's interest in removing personal data outweighs the public's interest in accessing his or her information under Article 11 of the CFR provides an individual with a prevailing right of removal.[107] But the court did not mention any tangible element to prioritize between 'public interest' and 'right to removal' when both public and private interests are competing though applicant's social position or applicant's public activities can generate public interest which can outweigh a right to be forgotten so easily.

Furthermore, another aspect pushes the controversy to another level which might occur through data controller like Google's responsibility to inform the third party (who hosts the data) under Art. 17(2) of the GDPR, of any possible erasure that the data subject apprehended and the subsequent effects caused by it.[108] The effects are essentially related with subsequent processing of the same data sought for removal. A case can be illustrated in this regard which occurred in the UK, in which Google already delinked his previous outdated conviction data

[101] Supra note 8, para. 14.
[102] Ibid
[103] Ibid para. 97.
[104] Ibid para. 85.
[105] Article 4(1), supra note 40
[106] Article 17(1), supra note 40, mentions the grounds of erasing personal data by controller.
[107] Supra note 8, paras. 94, 97.
[108] Neville, Andrew, Is it a Human Right to be Forgotten? Conceptualizing the World View, 15 Santa Clara J. Int'l L. 157, 2017. (Neville 2017)

from its database,[109] and informed the host of the content where the article was published.[110] Subsequently, the owner of the webpage produced another article with the notification of Google's removal from its search results along with the original story from the beginning about the applicant's conviction which drew attention of other media websites too and ended up producing more articles.[111] However, the applicant further requested Google to delink all the article links again but this time Google denied to do so on the ground of the news articles were new and of public interest.[112] Consequently, the applicant moved to the UK's DPO which is ICO with data removal request. The ICO took into consideration certain principles such as whether public figure, nature of data, time lapse, detriment of the data subject's reputation, graveness of offence and the involvement of journalistic material. While partially agreeing with Google, the ICO found that the news articles as newsworthy and of public interest, the ICO further stated that the public interest can also be mitigated without the name of the applicant which exposes him to his long spent criminal history.[113] The ICO found the articles to be excessive in relation to the purposes, pose disproportionate detrimental effect on privacy rights and cause the data subject anguish and ordered Google to delink the applicant's identity from the news articles.[114]

So, though there is a tension between public's right to access to information and individual's privacy rights, there are also certain principles applied by different authorities which might be helpful to get a direction of balancing norms.

3.2.2. Tension in balancing between public right to access to archived information and right to be forgotten

This second point of tension is derived from another lawful data processing exception which is data collection for scientific, historical research or public research purposes, and individual's right to delink that information. In *Google Spain*, the CJEU, while supporting to determine in case to case basis, ruled that the search engine data controllers can be obliged to wipe the links which lead anyone searching for information against a name to the site the data is hosted, under

[109] Information Commissioner's Office, Data Protection Act Of 1998 Supervisory Powers of The Information Commissioner Enforcement Notice 2015.
[110] Ibid at 14.
[111] Ibid, at 15.
[112] Ibid, at 19.
[113] Ibid, at 27.
[114] Ibid, at 29-30.

DPD.[115] Again, it did not outline exact elements when request of removal of these unwanted links shall be respected because public's right to access was already well established through law and case laws but right to removal was not. Thus, it left a tension between specific law and unspecific ruling though processing of data for archiving purposes in public interest, statistical, scientific or historical research purposes is allowed under data processing principles.[116]

While determining RTBF, the CJEU delimited the right within search only which is performed through the search engines, not broader which means that the delinking was only effected in search engine lists only while the information remained in other places online. Indeed, the information can be retrieved by going to the direct website or even by searching any other thing except distinct name or any other identifiable element of the data subject, for example, by home or official address of the convict or other data subject's name who did not apply for a RTBF. Consequently, the RTBF is defined as not total erasure of a data, rather, restriction in finding the data. That is coherent to earlier critics such as Markou's (2014) argument who argued that forgotten does not mean a total erasure of the data. According to a distinguished Internet scholar Roberts (2015), compared the scenario metaphorically by saying that it can be compared to making the catalog of a library disappear, while the book is unharmed, stays in the same place in the collection.[117] However, the analogy might seem to be not entirely right according to the findings of *Google Spain* since it more or less appearing that the books stay, so as the catalog, just an entry from the catalog is omitted, not the entire catalog. For better fathom, even the book remains in the exact place so as to say that if anyone knows the name of the author or category of the book, he or she can find it by going to the exact place. That is why Jimmy Wales opposed Google Advisory Council Report (2015, 27) which stated that exposer's actions 'are being suppressed' and said that the report is represents an exaggerated effect of RTBF[118], which is not true, in particular, not consistent with the actual effects of RTBF. However, other commentators are also available who supported the Advisory Council Report to an extent by saying that there should not be any distinction between data available in different sources such as files, archives such as newspaper, or government records which can be found through search engine searches Google Advisory Council Report (2015, 28).

[115] Ibid, at 100(3).
[116] Art. 5(1)(b), supra note 40.
[117] Roberts, Jeff John, The Right to be Forgotten From Google? Forget it, Says U.S. Crowd. Fortune, 12 March 2015. (Roberts 2015).
[118] The Advisory Council to Google on the Right to be Forgotten, Advisory Council 2015, available at: www.google.com/advisorycouncil/. (accessed on January 30, 2020)

This is in pessimism to the scholars like Mayer-Schönberger (2014) and Bernal (2011) who wanted to see a pure deletion or erasure through a successful exercise.[119] However, since the data is usually still available, any party with legitimate interest for example, if any bank is considering to provide a loan and wishes to look into a bankruptcy history, then it can perform a search by putting the loan applicant's formal name or anything else though it is not guaranteed that it will be able to find something even if, there is any data. The distinction is this case from the above case is in the former situation, the search example is general, but in the latter case a purposive search is performed. So, the ultimate balance is that total erasure was and never supported by the *Google Spain* judgment, and so the history or the data is intact online. Besides, whether the data subject's activities involve any public interest or not will be taken into account. According to Bernal (2011), the judgment failed to reach the milestone which many privacy advocates asserted to cross.[120]

3.2.3. Tension between different provisions of CFR

According to David (2014), the CJEU prioritized the RTBF in *Google Spain* case, while outlaying free expression right which also has the similar status in CFR and both are considered as fundamental principles after Lisbon Treaty.[121] The meaning of the sentence is clear and true to be interpreted but to some extent. Such a statement would need to be clarified since it completely overlooks principle of balancing under Union law. However, CFR protects the free expression right quite vastly, in particular, it does not directly allow free expression to be hindered by a RTBF.[122] But a limit on free expression on the basis of a RTBF can easily be accommodated through interpretation within the limitation sub Article of Art. 11. But the real controversial point is that though indivual data protection right is also ensured in CFR, it does not entail any other ground other than consent based processing and any other lawful way,[123] for example, under any of the grounds mentioned in Art. 6(1). Analogically, it does not purport to prioritize one right over the other.[124] It manifests equality over both the rights. But in *Google*

[119] Mayer-Schönberger, V. Omission of Search Results is Not a 'Right to be Forgotten' or the End of Google, The Guardian, 13 May 2014. (Mayer-Schönberger 2014) (accessed on January 30, 2020)
See also, Bernal, Paul Alexander, A Right to Delete? European Journal of Law and Technology 2 (2), 2011. (Bernal 2011)
[120] Ibid
[121] Google's Chief Legal Officer, David Drummond, We Need to Talk about the Right to be Forgotten, The Guardian, July 10, 2014. Available at:
http://www.unlock.org.uk/policy-issues/policy-cases/case-of-natasha-online-links-hampering-chances-of-promotion/ (accessed on 7 April 2018)
[122] Ibid.
[123] Article 8, CFR
[124] Charter, art. 8(1), 2012 O.J. (C 326) 391, 397

Spain case, it recognized the right in concern (RTBF) in the form of delinking to personal data over right to freedom of expression in the form of restricting right to access information. Consequently, it remained unclear whether data protection right is prioritized over publication right such as free expression under CFR when it comes upon the spent convicts. Though it is true that one right cannot exist without the other, Article 10 of GDPR provides special protection on data related to criminal convictions and offences.

3.2.4. Tension between GDPR and CJEU Practice on Privacy Rights

Right to be forgotten recognized by GDPR which can be considered as the second generation of this right as well as the second generation of balancing regime.

Article 10 of GDPR mandates the processing of personal data with a criminal offence records upon authorization of Union or Member State law only. Recital 19 of GDPR reaffirms the protection against processing of data regarding criminal convictions under specific Union legal Act though this enactment does not deal with this issue in particular. Furthermore, while outlining the derogations relating to the 'archiving purposes in public interest, scientific or historical research or statistical purposes', GDPR emphasizes on data minimization because of rights and freedoms of data subject.[125] It is to be mentioned that data minimization has been mentioned or already has the status of a monumental principle in data processing area.[126] To serve this purpose, pseudonymizing is mentioned as a tool so that data subject becomes unidentified. But in reality, maintaining consistency with Art. 10, the CJEU as an EU institution authorizes processing through its communication by publishing its rulings in form of press release which leaves room for tension in complying with GDPR with regard to privacy rights.

3.3. Different Approaches in Balancing and the Gap

This portion tends to analyze balancing approaches made by different sectors of competent stakeholders. In this section, based on core role players: the European Court of Justice approach, Scholar's approach and GDPR approach is analyzed and thus identified the gaps while discussing the approaches with two real life cases.

[125] Article 89 (1), GDPR
[126] Art 5(1)(c), GDPR

3.3.1. Mention of sources of approach and real-life cases

Easing tension or balancing the conflicting interests mentioned in the previous section can better be understood with real life scenarios of the victims who already spent their convictions or in the similar sense. In one prominent case, one claimant GC requested a link to be delinked from the Internet in which she is represented satirically with the city mayor to whom she served as a cabinet head to show the existence of an intimate relationship between them so that in the long run, she can derive political benefits.[127] The montage of the photo in question came into light when GC was running provincial election in which she was a candidate but ceased from performing in the previous job. In the second case, ED, the claimant, requested for delinking two articles disclosing his criminal history of sentencing seven years imprisonment and additional ten years of judicial overseeing for committing sexual offence against fifteen years old children.[128]

In addition there are some fictitious cases which are collected from different sources, mostly based on the UK such as guest speech of ICO's Data Protection Conference[129] and Unlock, an NGO who collects evidence of people who have applied for their "search results" to be removed by Google and others but failed.[130] First case is about Sonia (anonymized) who was convicted of Arson, spent conviction and was doing a job in a good pace. Her previous husband decides to destroy her after divorce and for that he prints off the newspaper article found in Google about her convictions and threatens to post everywhere.[131] Second case is about Natasha (anonymized), a school teacher convicted for four years of fraud in duty. Now after spending her conviction, she is again working with a school but in entry level. The employer informed her about less chances of progressing due to the possibility of backlash from parents of the children. All these happens because her conviction article is visible online.[132]

[127] GC, AF, BH, ED v CNIL Case C-136/17, paragraph 25.
[128] Ibid, paragraph 28
[129] https://christopherstacey.wordpress.com/2015/11/11/the-google-effect-criminal-records-and-the-right-to-be-forgotten/ (accessed on 15 May 2018)
[130] http://www.unlock.org.uk/policy-issues/specific-policy-issues/google-effect/ (accessed on 15 May 2018)
[131] Ibid
[132]http://www.unlock.org.uk/policy-issues/policy-cases/case-of-natasha-online-links-hampering-chances-of-promotion/ (accessed on 15 May 2018)

Now, based on the balancing approaches derived from the CJEU rulings, scholarly thoughts and the law, the following section will try to answer a logical issue in general. The issue is that whether the scope of *Google Spain* ruling demand all links connecting to the personal data to be obliterated.

3.3.2. Easing the tension between privacy rights and freedom of expression by different sources of implications

3.3.2.1. Implication of CJEU and ECtHR approaches in balancing privacy rights and freedom of expression

Easing the tension between publication right in particular right to freedom of expression and individual data protection right in particular right to be forgotten proved to be difficult as both has to accommodate each other as well as coexist. The CJEU approach in easing the tension is worth mentioning in this context because the honorable court tended to balance them in analogous dominations. Using the same mechanism might serve as derogatory grounds from freedom of expression for privacy right or right to be forgotten.

In *Bodil Lindqvist*[133], the CJEU stated that gauge of weighing between those contradictory rights race against each other within the ambit of the contemporary data protection enactment.[134] Specifically, the contemporary data protection law defined the scope of lawful and unlawful processing with a view to preventing illegitimate processing from happening or continuing under the native legal intellection.[135] Article 9 of the Directive then and now Art. 17(3) of the Regulation includes derogatory grounds that leave rooms for the Union Members to allow processing under any of those particular principles which is discussed broadly in the previous chapter. The purpose of providing the exceptions in the name of derogations are clearly stated in the DPD which is to ensuring the coexistence of both the rights through weighing each other in a particular situation.[136] It needs to be kept in mind that the mechanism of ensuring coexistence completely differ now and before when the DPD was operative. That is why in *Bodil Lindqvist* (2003) case, the CJEU instructed the Member States to make sure the enforcement of the weighing mechanisms through the exercise of their freedom of approach

[133] Sweden v. Bodil Lindqvist, Case C-101/01, 6 November 2003.
[134] Ibid, para. 82
[135] Ibid, paras. 82–90.
[136] Data Protection Directive, Art. 9.

manifested in the contemporary law.[137] It further added show persistency while weighing since the domestic courts were expected to balance the competing rights by relying on the primary principles set by the Union legal order.[138] In another Finnish case before the ECtHR, the honorable court found the necessity of unifying the approaches so that a better harmonization can be achieved through providing guidelines for weighing competing interests.[139] The judgment vigorously made it clear that none of the competing interests in particular, individual privacy right and public freedom of expression are exclusive, therefore, both of them can be restricted if appropriate reasons are found reconciled within the law, serve the purpose of providing rights and last but not the least are consistent with the democratic merits of a particular legal system or the society.[140]

Being a privacy right, this logic can be applied to the right to be forgotten. Turning to the abovementioned case of GC and ED, the CJEU interpreted publication or further processing of data and right to freedom of expression must exclude the processing of sensitive or special category of information unless otherwise is expressed in the law. It is to be noted that Article 9 of the GDPR defines special categories of data which are affiliated with expressing 'racial or ethnic origin, political opinions …'[141] In the case of GC, the article was associated with her political belief and orientation. Besides, the alleged relationship was not proven which makes it an inaccurate data which interfered with her privacy rights unlawfully. However, she was a public figure at the time of performing in city council, even at the time of the judgment she was a figure whose activities was related to public. To put it differently, the common people had an interest to know about her since she was running the provincial election. But the fact needs to be brought up that, not only the accuracy of the information is questioned, but also the information was brought to light in a crucial moment when she was running her campaign. Journalism is clearly in bad faith and to harm her public face which was not brought anytime before. Furthermore, she is not connected with her previous profession anymore. In that situation her privacy right should be respected in the event only the information about personal relationship is nothing but false.

[137] Supra note 133, para. 87.
[138] Ibid
[139] Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, Case 931/13, 27 June 2017, paras. 55–56.
[140] Ibid, see also, Art. 8(2),
[141] Supra note 127, paragraph 25.

Turning the situation in case of ED who was convicted for sexually abusing children under fifteen years of age. Article 10 of the GDPR clearly forbids the processing of criminal data without the control of the official authority. Even it says that any maintenance of criminal history database has to be under official authority. Though the law seems to be attracting a deletion of ED's conviction data, other factors compete to detract it. For example, the nature of the offence is gruesome. It might become relevant to the public as long his activities include the common public in general which will necessarily attract both journalism and public interest. For example, if at any time he starts performing duties with institutions which offer its activities to the children, then the common people having services from that institution have legitimate interest about the former criminal. It is well beyond to his right to privacy and data protection.

Now considering the presumptive case of Sonia, availability of her conviction story for arson presumably does not fulfill any journalistic, artistic or literary purpose anymore since the journalism purpose has been achieved already and so unavailability after a certain time would not frustrate any of the purposes anymore. Besides, if she does not play any public role, or takes part in any public activity then, her data attracts to be removed online to make her life easier by not providing a weapon of malicious defamation by her ex-husband. On the contrary, the news about the school teacher Natasha might be very crucial for journalistic and public interest purposes as she committed the crime in a position of trust and while involved in taking care of children who belonged to common people. So, *Google Spain* might not attract the situation as public has legitimate interest to know everything related to their children now and in the future since her conviction was against society specially when she was vested with official duty.

The balancing methods employed by the CJEU provide some guidance on the qualification of public interest but lack clear direction for the Member States since guidance does not cover all contemporary challenges raised after GDPR came in force. Rather it encouraged Members to strike a balance at some point against privacy interests which was against EU law harmonization.

3.3.2.2. Implications of scholarly opinions on balancing the rights at issue

First of all, Scholars are divided in describing the reach of RTBF. Some believe that the CJEU failed to ever establish the comprehension of GDPR, while other believe that it is the inception

of modern era of privacy rights.[142] Opinions of the scholars and advocates can be considered a great source for looking into the balancing approaches. Niilo Jääskinen (2014), the advocate general thinks that since the right to free expression attracts elemental safeguard within the Union legal system,[143] safeguards must be taken from putting the primary responsibility of shifting the balancing approaches to the data controllers such as the Internet search engines[144] or other data controllers, in particular, in cases of erasing a data or deciding right to be forgotten cases, though responsibilities have been vested upon the controllers under Art. 17(2) of the GDPR. He again tended to reaffirm the strong respect of freedom of expression in the EU while his concern about delivering discretion to search engine companies to decide whether data subjects will be allowed to have their right to be forgotten or not. In a nutshell, the Advocate General is particularly concerned about the greater power vested on the data controllers to take initiatives in balancing complex competing rights since great power demands greater responsibilities and the data controllers have the possibility to err in disposing their responsibilities for so many logical reasons for example, trying to avoid detrimental legal consequences anyway, exploiting more for their legitimate profit interests and some others.

In addition, Advocate General Szpunar opined in his opinion on case C-136/ 17 that the settled case laws of the ECtHR thinks that the ability of the Internet in terms of providing data storage and communication is outstanding which essentially provides enhanced access to the public to news and other information and thus, simplifying the publication of all types of information in general.[145] He further added that the ECHR not only applies to the data retained through the Internet but also to the ways and means through which it is communicated or sent or received.[146] However, while analyzing his opinion, he stressed on the fact that the journalism factor used by the journalists and the listing priorities performed by the search engines are completely different.

[142] Mundy, Simon, Asia Considers 'Right to be Forgotten' Ruling Prompted by Google, THE FINANCIAL TIMES, (Mar. 12, 2015). (Mundy 2015)
[143] Opinion of Advocate General Jääskinen, Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), May 13, 2014. (Jääskinen 2014)
It is to be noted that the Opinions of the Advocate Generals have non-binding effect on CJEU and they are produced independently.
[144] Ibid, para. 133.
[145] ECtHR, Times Newspapers Ltd v. the United Kingdom (Nos 1 and 2), 10 March 2009, CE:ECHR:2009:0310JUD000300203, § 27, and ECtHR, Ashby Donald and Others v. France, 10 January 2013, CE:ECHR:2013:0110JUD003676908, § 34.
[146] ECtHR, Neij and Sunde v. Sweden, application No 40397/12, §10, 19 February 2013.

Again, David (2014) while noting about balancing between public and private rights, stated that it is possible under the GDPR to show and interpret that the privacy interest of the individuals can poise the opposite interest of the common people.[147] The GDPR, the reformed version of the Data Protection Directive, limits a right to be forgotten when limitations are plausible for 'journalistic, artistic, or literary expression, for protecting the public interest in public health, or for historical, statistical, or scientific research purposes'.[148]

While perceiving disclosure of personal information as governmental and non-governmental, Jacobs and Larrauri (2015), stated that the European countries foster the protection of one's privacy through protecting honor and dignity from both types of disclosure.[149] They added that the disclosure of particular information may lead to the violation of privacy rights irrespective of the information's being true or spurious since the EU legal system never focused on a piece of information's being right or wrong, rather, in the event of a communication turns detrimental for others' image, the focus is drawn on if the processor of the data or the correspondent has a right to reveal the information or not.[150]

Turning into the cases both real life and fictitious, the majority of scholars indicate that GC, ED, Sonia and Natasha all can either qualify or disqualify a claim of right to be forgotten depending on so many factors. The most commonly overlapping opinion is that right to access information merits particular protection in the EU. On the contrary, historians such as Antoon De Baets (2016) opined that the scope of derogation from right to be forgotten should expand to all forms of expression. However, in my opinion, the latter opinion suggests no existence of right to be forgotten which is contradictory and obsolete with the Union legal system.

3.3.2.3. Harmonization through GDPR in pre-established rule of allowing the Member States to strike a balance

The 1995 Directive along with CJEU's empowerment provided the Union Member States with the freedom to choose appropriate approach according to their each domestic adherence with a view to ensuring the balancing between the rights in the event of there is a lack of synchronous guidance under the law, caused disharmonization of EU law. According to the highest court,

[147] Lindsay, David, The 'Right To Be Forgotten' in European Data Protection Law, in Emerging Challenges In Privacy Law, Normann Witzleb et al. eds., 2014, pages 290–337. (Lindsay 2014)
[148] Recital 51, Art. 17(3), supra note 40.
[149] Supra note 47.
[150] Ibid

Art. 13 of the Directive made the Member States free to formulate their own legislative acts to indicate the limitation of people's right to information.[151] Besides, the CJEU stressed on State involvements in performing the balancing tests. *Bodil Lindqvist* and *Satakunnan Markkinapörssi* have been discussed already above in this context. The CJEU confirmed in *Bodil Lindqvist* that the functionality of balancing between concerned fundamental rights are executed from the domestic enactments of each Member State which is responsible for redacting the Directive.[152] This is however confirmed again in another case in which the CJEU provided broad discretion to the Union Members to take account their culture and tradition for construing the rules and procedures in balancing rights.[153] Now, with the enforcement of GDPR, harmonization is achieved through the direct effect of this law. Consequently, frustration of disharmonizing derived from the Directive and established by the CJEU waved remarkably.

Hence, one of the greatest obstacles is that only one right has been recognized as one of the overriding justifications over right to be forgotten that is right to freedom of expression and information.[154] As RTBF has already been recognized by the CJEU and it is one of the privacy rights, the balancing mechanisms between privacy rights and freedom of expression can be a tool for now to overcome the situation. In this matter, GDPR's method for choosing between competing rights does not differ from those employed by the case laws though Recital 19 and Article 10 of GDPR jointly mandate individual's protection against processing of data regarding criminal convictions and offences under specific Union legal Act which derives its objective to balance.

Turning into the cases, GC and Sonia deems to be awarded with her right to be forgotten under GDPR since any of the overriding conditions of their right to be forgotten is presumably not satisfied. Even if, it becomes necessary for freedom of expression or journalistic or archiving purpose, then using pseudonyms would respect her rights and freedoms through data minimization under GDPR data processing principle under Article 5(1)(c).[155] Again, in the case of ED and Natasha, for sake of public interest, journalism and archiving; these cases might not attract right to be forgotten since public's right to access to information is necessary. People

[151] Institut professionnel de agents immobiliers (IPI) v. Englebert, Case C-473/12, 7 November 2013, para. 42.
[152] Supra note 133, para. 82.
[153] Supra note 138, para. 53.
[154] Supra note 147, Article 17(3)(a)
[155] Recital 19, supra note 40.

have legitimate interest to know on whose hand their children is being educated and raised. However, other competing interests will be adhered to the upcoming sections and chapters.

3.4. Contemporary Principles of Balancing in Motion

To summarize, the fundamental rights must be weighed against each other so that they can co-exist together. In that case, the highest Court showed greater importance particularly on weighing the legitimate interests of the public in a particular information sought.[156] For this reason, elements responsible for making a person public or private figure and what activities fall within the scope of public needs to be discussed as one of the implicated principles in the next chapter along with implications of other principles.

Analysing the previous discussion, it is ascertained that balancing between right to freedom of expression and right to be forgotten comprises balancing of multiple connotations. The substances are sometimes mentioned directly in law and sometimes derived from CJEU and ECtHR cases, and scholarly opinions. Ensuring proper balancing proved to be a herculean task due to several reasons among which the most important is that the principles are dynamic and function differently on a contextual basis. Though it found its inception in CJEU *Google Spain* ruling, it is materialized for the first time in GDPR altogether. Now, we will turn into identifying the active principles of balancing between RTBF and right to freedom of expression.

3.4.1. Lawfulness and unlawfulness of processing

The vagueness in balancing principle is analogously persisting under CFR and GDPR when it comes upon the spent convicts. On one hand, traits between Art. 8 (right to respect private and family life) and 11 (right to freedom of expression) of CFR remains in discomfort though the matter has been discussed in the earlier part of this chapter. On the other hand, Art. 10 and recital 19 of GDPR, vests responsibility on the data controllers to process data related to criminal convictions or offences only under official authority like the Data Protection Officer. But Art. 11 off the CFR allows to exercise freedom of expression regardless any frontier and public authority which clearly shows the complexity of determining lawfulness of a processing. Depending on the matters and principles at issue, it is clear that it is a matter of contextual

[156] Supra note 8.

determination only which has to be performed in compliance with the motives and provisions of the law.

The processing principles exercised by the CJEU, ECtHR and GDPR can be construed towards striking balancing mechanism through a gradual developmental framework. Because one thing in common among all the undertakings which is in accordance with law or the grounds of lawfulness of data processing. While setting out the parameter of lawfulness, the CJEU introduced terms like 'inadequate, irrelevant, no longer relevant, excessive with the purposes of processing'. Besides, both CJEU and the ECtHR legalized processing for archiving data for public use in conduction of scientific or historical research. The public protection is adhered by allowing processing on the ground of exercising freedom of expression too. And the public rights are protected if that is consistent with the principles laid down by the law, meets the objectives of fundamental protection and comport with the values of a democratic society. Now, the provisions of law are clear with the enforcement of GDPR which now defines the scope of lawfulness of processing in its specific Articles which are discussed elaborately in chapter two. However, in construing the principles of case laws derived from both CJEU and ECtHR in collaboration with the GDPR, certain principles clearly abrogated with the enforcement of GDPR which were appointed during the Directive regimen. For example, while prioritizing between public and private interest: both the instruction and discretion of the Member States to adopt national provisions in accordance with personal social values and traditions are eroded and ousted.

GDPR only broadened the scope from search engine to controller but did not mention any design who is responsible to cross check these balancing enforcements which should be efficient enough to respect the right to privacy and personal data of spent convicts in each case.

At this moment, though GDPR might be the hegemony of related lawfulness of processing, it lacks to stir the proper balance well with special reference to the spent convicts. It can be said for now that the ruling started filling the gaps through outlining principles, more needs to be done after the expansive provisioned enforcement of GDPR which is thoroughly discussed in the next chapter.

3.4.2. Countervailing public and private interests at stake

In terms of the apex court, it failed to formulate a test to prioritize among public and private interests when both interests are competing in the same litigation. This problem is still lurking specially after GDPR's allusion of freedom of expression as one of the derogations to right to erasure. It would be reasonable to say right to freedom of expression would remain backed up like antecedent. Express derogation from erasure on the ground of free expression supports that claim while it is also true that balancing is one of the objectives of GDPR.

Here the potential clash is again visible because GDPR mandates right to exercise of freedom of expression and information as one of the derogations of right to be forgotten under Art. 17(3)(a) of GDPR. According to Recital 19 and Article 10 of GDPR, one of the objectives is to protect the basic freedoms and rights of the convicts. Additionally, Art. 10 (2) of ECHR outlines protection of reputation and rights of others as one of the reasons of restricting freedom of expression. So, as long right to erasure or to be forgotten has the effect of protecting other's reputation and rights, balancing becomes inevitable since it might impose a restriction on freedom of expression which is not ensured in a comprehensive way because certain tensions are yet to be eased for better fathom. In this matter whether the present legislation encourages the removal of information needs to be discussed in the next chapter.

In addition, for the purpose of prioritizing free expression right over RTBF, the Spanish Tribunal Supremo *(Sala de lo civil)* formulated a justification test for determination through certain judgments. Being truth, newsworthy, and germane are the constituent elements of the so-called justification test.[157] Firstly, the processing is deemed to be justified even if a particular information is detrimental if the information concerned is true or the data is the outcome of someone's rational effort of determining the truth, or it is revealed in good faith. Secondly, newsworthiness is another criterion for an acceptable processing which is required to have connected with public opinion or public interest. However, a tendency of elaborating the term 'newsworthy' is visible to have a broader interpretation nowadays comparing to the past which facilitates news media to have expansive leeway in publishing criminal history though publication of any criminal database or any criminal database related to a specific case is not

[157] Tribunal Supremo (Sala de lo Civil) Oct. 16, 2008 (No. 948); Tribunal Supremo (Sala de lo Civil) Oct,28, 2008 (No. 1013); Tribunal Supremo (Sala de lo Civil) Dec. 23, 2009 (No. 868); Tribunal Supremo (Sala de lo Civil) March 9, 2010 (No. 155); Tribunal Supremo (Sala de lo Civil) Apr. 28, 2010 (No. 264).

allowed. Lastly, it has to be studded with a news story which has been published earlier and needs to be published or processed to form an important part or complete the story.

To make it clearer, neither distinction between acts of public's interest and private interest, nor acts that fall within the ambit of those two competing interests have been revealed yet. The reasons are unclear on why public motivate their interest on an act which is private in nature. So, what are the factors which make certain acts or certain personalities public? These are not convened neither in any case law, nor in GDPR though both the GDPR and some of the case laws mention some of the components in some names associated aimed at journalistic, research, historical and archiving endeavors, but did not categorize directly between public and private interests. The same goes with the principles responsible for the construction of public and private individuals: by character or by activity? So, matching the balancing puzzles through discussing the evolving norms of both the public and private interests will be adhered in the next chapter.

3.4.3. Achievement of purpose

The terms used by the honorable ECJ in *Google Spain* stating 'inadequate, irrelevant, no longer relevant, excessive with the purposes' of processing literally indicates that there is a point when the purpose of the processing is achieved for instance, when a person is convicted of assault and battery. It can be assumed that after a certain period of time, the news or information becomes irrelevant to continue processing for journalistic or any other overriding purpose which means that further processing might be detrimental for the concerned individual's privacy. It also might be the case where limited processing of the data continues, for example, if the case is being appealed and the previous data is being referred in situations where issues emerge. The purpose achievement situations are seen in *Google Spain* where the court judged against further processing in fulfillment of the purpose. Even purpose limitation has now become one of the fundamental principles of data processing in the EU. Data with special reference to data related to spent convictions and offences are not allowed to process without consent or under authority. However, there are justified grounds when data continues to be processing even after main purpose such as journalism is achieved but secondary purposes are yet to be achieved such as for employment in concerned places. But what happens with those conviction data which can never be processed such as revealing witness identities irrelevantly? or which never fully achieve the purpose of processing due to having public interest? or what

happens even if achieved the purpose of processing, but availability of data is necessary for greater public interest? All these questions will be tried to be answered in the next chapter.

3.5. Conclusion

To conclude, both the CJEU and scholars agree at some point that balance is needed between the right to be forgotten and the freedom of expression.[158] But the complication is to balance the persisting issues enshrined in CJEU's *Google Spain* decision which caused tension among these two rights' elements. Historically, the right to be forgotten remained vague in its essence for certain reasons. Firstly, the ECJ did not decide how much weight one right should carry against the other. Secondly, the ECJ only ruled for search engines like Google, Yahoo, Bing and some others to delink the information where the original content remains with the publisher website. The obvious reasons for that might be the strong mandate and established respect for right to freedom of expression and maintaining availability of information in some way so that they are not lost forever. Fortunately, now the GDPR tackles both the problems in theory by specifying something to talk about while making data controllers liable for complying with the provision.

So, balancing has just entered into youth after surviving infancy and youth maintains considerable lacunas in defining and interpreting principles. However, existing mechanism of balancing is still working but not diligently as the rights are guaranteed. Since upholding fundamental rights is one of the mandates of EU legal framework, more visible protection is indispensable. To put differently, balancing is in its second generation and we need to push it to third generation for more tangible norms. For this, the identified areas need to be settled down in the next chapter while fragmenting and elaborating the elements of each principles to empower the balancing with those necessary fundamental tangible principles which are the imminent tools of allowing right to be forgotten in spent criminal convictions.

[158] Supra note 8, para. 85. Focus of the discussion was on how Art. 9 of the DPD weighed between individual privacy right and publisher's publication right.

CHAPTER 4: WAYS ON HOW IMPLEMENTATION OF BALANCING PRINCIPLES CAN BE ACHIEVED

4.1. Introduction

Multiple balancing principles have been identified for determining a right to be forgotten case. These principles are not derived from the law only, but from the interpretation and scholarly opinions of the law. Again, the principles did not emerge in a day, rather, those are the grains of almost a decade yielded by different laws, courts and scholars of the jurisdiction. Among the principles, the first one that comes into consideration is that whether the concerned processing has been done on the basis of any of the legitimate grounds of law or not. Generally, considering the amount of both legitimate and illegitimate grounds of processing, it can be said that both cover broader scope. That is why balancing is unavoidable in all cases. There are publication interests for the data controllers, on the other hand, publication interest can be contested by the privacy right holders. After apprehending a balancing approach, it can only be said whether a right to be forgotten can be granted or not. Now in this chapter, the balancing principles will be discussed thoroughly to have an insight of their discharging components.

4.2. Implementation of Balancing Principles in Spent Criminal Convictions

The balancing principles are necessarily identified to balance between publication and privacy interests in a broader context. The principles that will be analyzed here are: lawful vs. unlawful processing, public interest vs. legitimate interest, public vs. private figures, processing interests vs. personal interests, purpose achievement and passage of time.

4.2.1. Lawful processing vs. unlawfulness processing

4.2.1.1. Lawfulness of Processing

Processing of personal data associated with criminal convictions and offences is directly dealt in Article 10 of the GDPR. The language of the Art. 10 clearly shows that personal data related to criminal convictions or offences has been considered as sensitive form of data under GDPR which needs comprehensive protection. Any processing of this type of data might be unlawful if that is processed without consent, or any other unlawful manner. The law itself does not support the processing of these sensitive data in any manner which is open and at will. This provision requires certain conditions to be filled in order to support the processing of data

related to criminal convictions or offences, namely: 1) data to be processed only on the basis of 'lawfulness of processing' principles under Art. 6(1); 2) Processing has to be under official authority if that has not been authorized by Member State or Union law[159] under the data processing principle which is analyzed in cooperation with Article 5(1)(e) in the next paragraph; and 3) Extensive register of criminal convictions must always be entrusted only under the control of official authority[160] under data processing principle which is discussed in collaboration with Article 5(1)(f). Now the requirements discussion will turn to define unlawful processing under Art. 6 and data processing principles under Art. 5 consecutively.

Unlawful processing can be defined as any processing that cannot be justified under any of the grounds of Art. 6(1). So, in order to be a legally processed data, it has to be processed on the basis of one of the grounds: the data being processed on the basis of data subject's consent for a specified purpose or purposes[161], or for the execution of contractual liability where data subject is one of the parties[162], or controller is processing for complying with its legal requirements[163], or for protecting any emergent interest of the data subject or of other natural person[164], or processed in relation with public interest concerning matters affairs or under appropriate official duties[165], or processed for any lawful interest borne with the data controller or of any third party unless and until the interest is overridden by data subject's right to protect his or her data[166]. So, if the data is not processed on the basis of any of the above-mentioned grounds of this paragraph, the data shall be deemed to be processed illegally or unlawfully which perfectly collaborate with the data processing principles under Art. 5 of GDPR.

Analyzing data processing principles under Art. 5, it is found that both the set of Recitals and Articles discussed in the previous two paragraphs are the accurate shadow of the data processing principles. Firstly, in determining the manner of data processing which needs to be lawful, fair and transparent[167], data is prescribed to be processed with lawful consent of the data subject. Besides, if the consent is obtained from any child under the age of 16 meaning the data subject being a minor under this legal instrument, the consent has to be obtained from

[159] Article 10, supra note 40.
[160] Ibid
[161] Article 6(1)(a), supra note 40.
[162] Article 6(1)(b), Ibid
[163] Article 6(1)(c), Ibid
[164] Article 6(1)(d), Ibid
[165] Article 6(1)(e), Ibid
[166] Article 6(1)(f), Ibid
[167] Article 5(1)(a), Ibid

its (the minor's) legal natural guardian. Unlikely, if the consent in respect of a particular data processing is revoked, or upon a successful exercise of a right to object, the processing of that specific data should be stopped. Secondly, the data has its purpose limited for processing.[168] While achieving the consent, the processor of the data is supposed to clarify the purpose of processing as well. The data is not allowed to process beyond the specific purpose for which the consent was obtained from data subject. However, data processing will be deemed within legitimate purpose if that is processed for achieving any purposes in the fields of public interest, scientific or historical research or statistical purposes, for execution of contractual liability on behalf of both the data subject and the controller or other legal obedience of the data controller.[169] This is also added as one of the derogatory grounds of allowing right to be forgotten in Art 17(3) of GDPR. Thirdly, even if the data is lawful for processing, the data has to be processed in a finite scheme which is called 'data minimization'. In this principle, the data has to be processed only when it is adequate, relevant and restricted in connection to the purposes for which they are processed.[170] To make these clear, the right to be forgotten context in *Google Spain* case need to be illustrated where the honorable court applied data minimization principle by mentioning that on the event of the information's being 'inadequate, irrelevant or no longer relevant, or excessive in connection with the purposes' of the processing at issue made by the data controllers, the data has to be removed. So, the processing needs to be weighed against the purpose for which it is sought and only permissible if the processing becomes adequate, relevant and earmarked with the purpose and again the purposes can be related with 'public interest, scientific or historical research or statistical purposes', for execution of contractual liability on behalf of both the data subject and the controller or other legal obedience of the data controller under Art. 17 (1) and Art. 6 of the Regulation. Fourthly, in maintaining the accuracy of the data, law requires to maintain up to date data and again it has to be connected with the purposes of the processed data, if necessary, delete or rectify to maintain the accuracy of a specific piece of data.[171] Successful exercises of objection rights or RTBF by data subjects can serve as tools of maintaining data accuracy through erasing or rectifying a particular data. This principle also sought in *Google Spain*, where the applicant successfully established his right to object though it was under the Data Protection Directive. Fifthly, the data which identifies any person, for example, in the name of a particular person,

[168] Article 5(1)(b), Ibid
[169] Ibid
[170] Article 5(1)(c), Ibid
[171] Article 5(1)(d), Ibid

shall not be retained no longer after the purpose of the specified processing.[172] So, time limitation along with purpose limitation is adhered in here and so, after that time, the data is forbidden to retain with data subject's name or other identifiable recognition[173]. The CJEU used this notion in defining a case of right to be forgotten in *Google Spain* by saying that a RTBF is exercised when a search engine operator erases the links published by third parties which contain certain information about the individual, from its list of results when any search is initiated on the basis of that individual's name. However, processing is allowed if the data is stored for archiving purposed in public interest, scientific or historical researches or statistical purposes but subject to technical and organisational monitoring which support the last principle of processing which is to process with 'integrity and confidentiality'.[174] Additionally, technical initiatives by appropriate authorities for the security of data can also be sought for the protection against any unlawful processing and accidental loss or any form of destruction.[175] Last but not the least, the data controllers have been held accountable for complying all the data principles.[176]

Furthermore, 'Pseudonymization' is provided in Article 89(1) as a tool of complying with both storage limitation and data minimization principles. In this way the data can not only be preserved without tampering with the original source while maintaining the privacy of the data subjects but also it can serve as an appropriate tool for different stakeholders of spent convicts which are discussed broadly in the forthcoming chapters.

Data controllers are empowered or made accountable to exercise their discretion[177] on the basis of legitimate grounds whether to approve or disapprove any such request upon fulfillment of certain requirements mentioned in Article 21(1) of the GDPR. However, the liabilities of controllers in cases of approving data subject's request of exercising RTBF related issues such as using attainable technological measures, expense of enforcement and some others under Article 17(2) of the GDPR are not a subject matter neither of this chapter, nor of the paper. Rather, this paper intents to identify and analyse the principles of RTBF which remain dynamic altogether with each other and the wheel moves towards settling right to erasure cases.

[172] Article 5(1)(e), Ibid
[173] Ibid
[174] Article 5(1)(f), Ibid
[175] Ibid
[176] Article 5(2), Ibid
[177] Ibid

4.2.1.2. Unlawfulness of processing

No longer relevant and excessive in relation with purposes

One of the complicated phrases are not having relevancy anymore. The phrase is very easy to say but to implement. Derived from the purpose limitation principle of the data protection law, the essence is to have the data deleted when it is inconsistent with the primary objective of the *prima facie* data collection. However, for further processing purposes, data can be retained in the events of processing for secondary usage such as for archiving for historical or research purposes, detection of fraud or assessment of other risks by the government.[178] However there are challenges in ensuring the deletion or concealment of data. One of the reasons is that nowadays data is being collected for opaque purposes in the name of data mining.[179] The rationale behind it is that mining of extensive is capable of showing a trend which is useful for a novel knowledge. The phenomenon is well understood by the idea of 'functional creep'[180]. The notion essentially refers to a situation when a data is collected for serving a particular purpose, but later on it gets involved to serve another purpose, which is completely different.[181] Concern related to functional experienced a sharp rise from the early 90's, the dawn of emerging the Internet. Nowadays, the concern reached its peak for using the data for other purposes which is totally different from the mentioned original.

So, if there are data which are no longer relevant qualifies for removing or concealing it under RTBF claims, then the questions like when and why it is inevitable to submit a RTBF claim. The damaging point might be an issue when a data subject can be made aware and conscious about any existence and processing of outdated data which are no longer relevant. If the damage is already done, then it is definitely too late, and the measures can be taken on the basis of *ex post* undertakings which means data is being processed excessively in relation with the purpose. On the other hand, if it has to be impeded then the right must act to take *ex ante* undertakings such as through government systems that ensures that the controllers erase or minimize the data that are no longer necessary to retain, that might take place automatically after the passage of the expiration date fixed by the law. The *ex post* approach essentially refers

[178] Supra note 24, page 244.
[179] Ibid
[180] Clarke, R. Tax File Number Scheme: A Case Study of Political Assurances and Function Creep, 7 Policy (4), 1991. (Clarke 1991)
[181] Curry, MR. et al. Emergency Response Systems and the Creeping Legibility of People and Places, 20 The Information Society, 2004, page 362. (Curry 2004)

to the situation when the processing is continuous excessively for other purposes which is different from initially declared purpose. Again, the *ex-ante* approach is not expected to be generic since there are cases where RTBF contradicts with its limitations in the name of secondary or recent purposes. At this moment the *ex post* approach takes the lead when excess processing takes place and continues to damage the privacy rights which is connected to 'functional creep' which usually errs to the side of further minor processing.[182]

Thus, a RTBF claim on the basis of purpose limitation principle does not always succeed. However, it might provide a *locus standi* for exercising right to object which might stop further processing but not the erasure or delink from the search engines. However, generally when the data becomes irrelevant still not clear. Particular time frame such as after five, ten- or twenty-years data concerning the convicts can be irrelevant though processing might attract legitimacy anytime afterwards at another unspecified time if it becomes relevant again for example, if once spent criminal wishes to run for an election.

Irrelevant

In determining irrelevancy of a data, the CJEU stressed on looking into inaccuracy of a data relating to a data subject. For this, in Case C-507/17, while defining the territorial applicability of the RTBF, the CJEU ruled on indicating Member States for ensuring an achievement of rectification, erasure or even blocking from data controllers, in particular, when the particular data is inaccurate or provides a misrepresentation of the data subject.[183] Relevance with the purpose might be the most subjective issue in determining a RTBF case since to whom other than the data subject the information might be relevant, needs to be assessed in each case. In deciding the issue of accuracy of data, Judge Warby found in the case of NT1 that with regard to the claimed words and phrase to be inaccurate, no evidence was provided on behalf of the claimant to prove the facts to be inaccurate. Rather when the judge understood the facts and interpreted in the context of another case[184], the claimant tended to exaggerate his claims by supporting his representation of self which led the judge to decline his claim of being the data to be inaccurate.[185] On the other hand, in case of NT2, the claimant argued that the fact that the claimant gained financial benefits from his criminal activities to be inaccurate and the court

[182] Supra note 24, page 244
[183] Supra note 58
[184] On the basis of the case Charleston v New Group Newspapers Ltd [1995] 2 AC 65.
[185] NT1 and NT2 v Google and The Information Commissioner, 2018 EWHC 799 (QB) at 83, 142.

also found that to be true in the light that it provides a misrepresentation of the data subject and made an order of delisting.[186] So, mere claim of inaccuracy is not enough, in what context it is inaccurate needs to be evaluated to determine having legitimate interest. Both legitimate interest and accuracy or relevancy related to a specific purpose is derived from context.[187]

Inadequate

It is undeniable that the term 'inadequate' is highly controversial due to its level of perception. What is inadequate for someone might be adequate for others. That is why what is inadequate online needs to be determined by the appropriate authorities. However, certain cases such as child pornography, or revenge porn and some others can be said adequate or inadequate instantly in terms of determining whether something happed or not. Again, inadequacy can well be determined in cases where someone gets acquitted but only information appears till bringing of charge against when a search is conducted. It is unclear that to what extent an inaccurate information may lead to inadequacy[188] because in most of the cases, the common element is defamation and the data controllers have less interest in conducting any background check of the data subjects before processing. Even data controllers such as search engine providers do not distinguish between personal data and other data. In that situation, there is no opportunity to presume that the claimant has any kind of face value. It should be the responsibility of law enforcement bodies from data controllers to CJEU to determine whether the data in question is inadequate with regard to the purposes or not.

4.2.2. Public interest vs. legitimate interest

4.2.2.1. Public interest

Public having interest in accessing a data plays an outstanding role in balancing fundamental rights in particular privacy and publicity rights. That is why while interpreting public interest, it needs to be delimited what it actually means since only the accuracy of the information processed disseminated online does not amount to befit to avert any other civil or criminal liability.[189] In this consciousness derived from both civil and common law legal system,

[186] Ibid, at 191.
[187] Gratton, Eloïse and Polonetsky, Jules, Privacy above all other Fundamental Rights? Challenges with the Implementation of a Right to be Forgotten in Canada, 28 April 2016. (Gratton and Polonetsky 2016)
[188] Supra note 74, page 15.
[189] Société TVA inc. v.Marcotte, 2015 QCCA 1118, para. 99.

individual privacy rights can better be protected within Union framework if the norm is established that the concerned information processed publicly not only needs to be true and accurate but also it must convey the specific subject matter in which the public has a 'legitimate interest'. Professor Trudel marked the term as an emerging and complex one. In his book he described 'public interest' is such as term which is attributed to be defined by many disciplines of human science related to fundamental thoughts and actions related to human behavior such as morality, human ideology, common beliefs and other realizations connected with the civil societies.[190] In simpler sense, the common sense and ethical value of the connexion era determine the rationale since no other law is able to impose any mastery over the value which regularly contradicts and changes. Having a refined view of the concept, the value is essentially connected with settling what the mass people is empowered for to ingress into or have a clinched gusto in knowing within the society in which other concepts can compete with each other furiously.[191]

Some common law perceptions are worth mentioning in this circumstance. Justice LeBel stated that the definition of public interest differs contextually. However, the notion actually means the publication of information has not to be performed only to satisfy the quench of 'media voyeurism', rather, the purposes needs to be connected with a certain degree of societal aptness, or the privacy right will be considered violated.[192] Again, in *Grant vs. Torstar Corp*[193] Chief Justice McLachlin stated certain scenarios that a matter can be considered as of having public interest. That is in order to consider an issue whether it has public interest or not, the matter has to be the one which attracts attention from the public, or in which the common people shows genuine concerns due to its affecting the wellbeing of the residents, or any act involving nonnegligible, disgraceful or scandalous in nature. He further added, that the data subject who has been referred in a communication must have a public function primarily, and only having sensual interest is not justified. Some portion of the public needs to have a natural interest in learning about the information came to light.[194] Undoubtedly, this will enhance personal data protection adherence to a greater extent.

[190] Trudel, Pierre, L'oubli en tant que droit et obligation dans les systèmes juridiques civilistes, 2013. Unpublished work prepared for the course in cyberlaw, Faculty of Law, University of Montreal.
(Trudel 2013).
[191] Ibid
[192] Société Radio-Canada v. Radio Sept-Îles inc., 1994 CanLII 5883 (QC CA).
[193] Grant v. Torstar Corp., 2009 SCC 61, at para. 105.
[194] Ibid

4.2.2.2. Legitimate interest

There are fundamental differences between the US and the EU in terms of role played by electronic and print medias in terms of disclosing criminal conviction data disclosure. In the EU, criminal documents such as judgments as its intact form is not available publicly so that anyone can inspect data with individual identities. For that interested person or entity needs to prove having 'legitimate interest'. However, the researchers, or common people, or the public watchdogs are able to have insights of the roles of law enforcement agencies, public prosecutors or even court proceedings in any case or a particular category of cases such as cases related to bankruptcy, corruption, or even geographical location, or related to politicians. For example, in Spain, the judgment of a particular case is served to the case parties only, not communicated in an open court except certain extremely notorious matters attracted by the wide media coverage subject to huge attraction of public interest.[195] The lower courts are also directed the same. However, the highest courts bring them to light after anonymizing the personal information of the parties through the intervention of the Centre of Judicial Documentation (CENDOJ) which is responsible for anonymizing the personal data of the defendant, as well as the witnesses and the complainants.[196] To challenge the case finding matters, the cases in Spain are searched by the date and name of court which is highly unlikely in the US where a case is searched particularly by the defendant's name[197] which shows strong Spanish constitutional adherence for the rehabilitation of the convicts.

Besides, in the UK, in a particular case[198], in determining the issue whether the facts caused unlawful interference with privacy or not, against the claim of NT1 which was that the availability of the information caused serious damage to his subsequent behavior as a 'pariah' in his personal and professional life, even having menace commonly[199], the court found that even though there were some sensitive health data, the information was made open in a the same transaction of disclosing such data which are not private at all[200] supported Google's view that NT1 remained associated with the same type of business activities in which he committed fraud and was convicted and confirmed that the information is allowed to be online so that common people can seek a correction on what misleading representations NT1 was making

[195] Supra note 47.
[196] Ibid
[197] Ibid
[198] NT1 and NT2 v Google and The Information Commissioner, EWHC 799 (QB) 2018
[199] Ibid, at 149.
[200] Ibid, at 140, 145, 146.

after his sentence became spent.[201] On the contrary, in NT2's case, the court found that the inaccurate information of gaining money from his conviction was indeed making trouble for NT2 in having any banking amenities as well as business adhering which is amounted to having illegitimate interest.

For the journalists, Jacob and Larrauri (2015) believes that reporters are free to consult or interview different stakeholders of a criminal proceeding for instance, investigating officers, judges, prosecutors, defence lawyers, if necessary, witnesses, victims, defendant or even prison staff in order to discover any arrest or accusation. However, European newspapers are not allowed to publish anything at their sweet will because there is a risk of violating criminal record confidentiality right.

4.2.3. Public vs. private figures

Distinguishing between public and private figures have become of high importance since it's being having role in determining RTBF case. Derived from the DPD and the *Google Spain* case, the CJEU stressed on the applicant's being a public figure and indicated the possibility of denying the application for delinking the subject matter. In having insights into public activities, the following can be seen. While balancing privacy and public interest, the judge focused on the Article 29 guidelines in the case of NT1 and NT2[202] and opined that in the case in which NT1 is the claimant, was still involved in similar financial activities relating to lending money to other business and individuals prior to his conviction and added that since he was involved with a grave offence and his own portrayal aimed at public, he is considered a public figure and public has all legitimate interests to be informed of his false and misleading representation of own.[203] To the contrary, the court found that though NT2 used to be a public figures, after his conviction became spent, he was not associated with the same type of business activities, and he pleaded guilty in the first instance, and lastly all relevant data was not seeking for hiding his criminal activities, his right of reformation was justified and his information relating to having financial gain did not attract any public interest.[204]

Public figures can be defined as those people who plays their roles in a society as politicians, celebrities, other online personalities, or even leaders in particular areas who possess a social

[201] Ibid, at 117.
[202] Ibid
[203] Ibid, at 130, Ibid, at 139; See also, Von Hannover v Germany (No 1) (2005) 40 EHRR 1, at 63.
[204] Ibid, at 205 and 206.

position in their respective areas and the ability to influence and has a public role to perform.[205] Coors (2006) categorized public figures between two categories: absolute and relative public figures.[206] According to the writer, absolute public figures are determined on the basis of their eminence, whose fame is well known to the common people because of their position, relevance and public activities, for instance, politicians, celebrities, monarchs .... .[207] De Baets (2016) believes that exclusive public characters such as politicians, monarchs or celebrities dispense a disproportionate effect on a society because their activities allure the common people which attract remarkable media coverage.[208] He further believes that absolutes figures control their affairs and activities online more strictly as they release and dispose their activities by staff and limited means.[209] However, it is highly unlikely that absolute public figures who spent their convictions tries to exercise a RTBF because it might backfire to the intention of removing data online due to public's curiosity and interest to know anything about their renowned individual. Later on, it might end up in having the 'Streisand effect'[210] with larger circulation.

Besides, relative public figures are determined as those personalities whose reputation relies on a specific event, for instances, a heinous crime or important public trial.[211] Relative figures gain attention abruptly and it may not be permanent. For those who study and rely on statistical or empirical data, studying relative public figures are necessary for two main reasons: for deriving anecdotal cases and for showing trends and aptitudes.[212] The purpose of the former one is to serve the journalism purposes as well as entertainment of the readers and the latter illustrates specific trends within the society, for example, trends towards crime or racial discrimination. Both ignite public interest to have clear-sightedness so that knowledge can be

[205] Ferrari, Anne, Using Celebrities in Abnormal Psychology as Teaching Tools to Decrease Stigma and Increase Help Seeking. Teaching of Psychology. 43 (4), 2016, pages 329–333. (Ferrari 2016)
[206] Coors, Corinna, Headwind from Europe: The New Position of the German Courts on Personality Rights after the Judgment of the European Court of Human Rights. German Law Journal 11 (5), 2010, pages 531–538. (Coors 2010)
[207] Ibid
[208] De Baets, Antoon, A historian's view on the right to be forgotten, International Review of Law, Computers & Technology, 30:1-2, 2016, pages 57- 66, (De baets 2016)
[209] Ibid, page 60.
[210] The term is hatched in 2005 after the name of Singer Barbra Streisand. It is a phenomenon where attempt to hiding or removing… results in greater spread. See also, Cacciottolo, Mario, "The Streisand Effect: When Censorship Backfires. BBC News, June 15, 2012.
See also, Parkinson, Justin, The Perils of the Streisand Effect. BBC News, July 30, 2014. Available at: http://www.bbc.com/news/magazine-28562156. (Parkinson 2014) (accessed on January 5, 2020)
[211] Supra note 205.
[212] Ibid, page 60

acquired in concerned matters so that preventive measures can be adopted in due time. The relative public figures suddenly fuel news columns and indicate issues of public debate.[213]

In contrast, figures unknown to the common people, are defined as the private figures.[214]

Now, turning the discussion towards spent convicts, who can be either absolutely public, relatively public or private figures. The level of protection for all types of applicants are reasonably not the same. In deciding the level of data protection, the ECtHR adhered to very careful interpretation which provides the least privacy protection to absolute public figures among all due to their prominence, then to relative public figures, then to private figures.[215] That means politicians, monarchs, celebrities enjoy have the minimum privacy spheres in contrast to the private figures who enjoy the largest ambit of data protection rights. And relative public figures lie somewhere between the highest and lowest data protection sphere, nonetheless, the absolute public figures also relish to a certain degree of privacy rights since the right itself is universal and applies to everyone.[216] While stressing on the 'reformed sinners', Joel Feinberg (1975) urged the plea to leave them alone particularly even when the newsworthiness is allowed or not in the future, when the relevant data subject wishes to get admitted in the sphere of private figure from spotlight where he came once involuntarily, and it should not hinder the rehabilitation process in the new life where privacy interest outweighs the publication interest on true facts.[217]

So, what remains is that at some point, absolute private figures can turn into relative public figures or even private figures. Anyone intending to exercise right to freedom of expression, performing newsworthiness, or defining any pattern can treat those data in an anonymous way in the figure dependent way which would suffice the purpose.

4.2.4. Processing interests vs. personal interests

4.2.4.1. Processing interests

[213] Ibid
[214] Ibid
[215] Supra note 203, See also Coors, supra note 206, page 537.
[216] Supra note 207.
[217] Feinberg, Joel, Philosophy of Law, Limits to the Free Expression of Opinion. Belmont: Calif, 1991. (Feinberg 1991)

History, statistics and research

During the draft presentation of the regulation, Justice Commissioner Reding confirmed that the RTBF is nonexclusive in nature and emphasized further on keeping databases with special reference to newspaper archives.[218] The regulation itself set the RTBF exemptions for 'historical, statistics and research purposes'. To meet that objective, spent convict's data can be retained in anonymized form to the highest extent possible. In *Google Spain*, derived from Art. 6 of the DPD, the honorable court also mentioned that any processing performed for of 'historical, statistical and research' purposes are not in contradiction with the law. However, the court also stressed importance on implying appropriate safeguards against any possible abuse of the provisions by the Member States.

Internet archives

It is apparent that the landmark *Google Spain* case consulted the phenomenon of linking data subject with his identifiable defamatory information retrievable from the Internet archive. The archive can be understood as permanent and temporary basis. The compilation of the information that is available in different third-party websites are permanent. On the other hand, while showing as the temporary archiving list, search engines play the primary role in fetching that information altogether in specific consolidated archived manner. In most cases, the data subject requests the expulsion of those links from the search engines' temporary archives which appear as results which assist to lead the user to the permanent archives. Though it showed to have adverse impact on reformed sinners, the CJEU reaffirmed Internet archives as the inexorable tool of history writing.[219] In 2009, the ECtHR agreed on the substantiality that

> ''Internet archives have … to avail news… such archives are important sources for education and historical research… primary function of the press in a democracy is to act as a public watchdog… it has a role in..
>
> However, the margin of appreciation afforded to States in striking the balance between the competing rights is likely to be greater where news archives of past events, rather than news reporting of current affairs, are concerned. In particular, the duty of the press to act in accordance with the principles of responsible journalism by ensuring the

[218] Memo: Data Protection Day 2014, Full Speed on EU Data Protection Reform. European Commission, 2014. (accessed on July 17, 2019)
[219] Supra note 8.

accuracy of historical, rather than perishable, information published is likely to be more stringent in the absence of any urgency in publishing the material''.[220]

So, while acknowledging the importance of the Internet archives, the honorable court also vests extraordinary responsibility on the press in maintain the accuracy of any information. The necessity of maintaining the informational integrity in Internet archives is even agglutinated in 2012 by the French *Court of Cassation* in order to ensure individual's right to be forgotten. In its case number 5525, the third section of the French court stipulated that Internet archives maintained by newspapers, in this case, the Italian one named *Il Corriere della Sera* should be updated with the compliance of Art. 6(d) of the Directive 46/95/EC which obligates to keep personal data in 'accurate and updated form'. The logical interpretation behind that is clear which is to fostering right to erasure by implementing the delinking upgradation beyond the search engine level, by applying it in third party level and even if I think, the information is kept anonymized, the exploitation and the utility should remain the same for the public.

Jacobs and Laituri (2012) argues in this regard that the European legal system considers the data relating to criminal convictions as 'personal data' which have to be treated confidentially.[221] The Union law forbids the idea of creating individual criminal records which can be identified by data subject's name through its adoption of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data[222] and Art. 8.5 of the DPD. Consequently, unlike the US, there are no commercial entity in the EU who is able to sell personalized criminal conviction databases.

4.2.4.2. Personal interests

Charge is on individual data subjects

From the beginning of the right, the common trend that has been developed in such a way which puts the responsibility on individuals who is concerned for his or her privacy rights (Van der Sloot 2014). In this sense, it is the data subject who is a natural person, who is vested with the onus of showing that particular URL or URLs are violating their data protection right so

[220] Times Newspapers vs. United Kingdom, (applications 3002/03 and 23676/03), §45 2009.
[221] Jacobs, James B. and Larrauri, Elena, Are criminal convictions a public matter? The USA and Spain. Punishment and Society 14(1), 2012, pages 3-28. (Jacobs and Larrauri 2012)
[222] Signed January 28th 1981; ETS (nº 108),
available at: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm. (accessed on January 5, 2020)

that the data subject can claim a RTBF. The fact is also true that if others are particularly keen in finding injururious information about the data subject, they can spontaneously retain the so called outdated or excessive data about the data subject which might come to light afterwards. The bonds of the Web can find and present it in so many contexts which might repose the threat again. So, the problem is not the URL, but the information which is brought by the URLs and individuals can keep a track of the dissemination of the URLs on which the information appears and contact the data controller. For this reason, it does not deem to be so easy to get rid of from all the information in cases it is disseminated broadly (Jones 2015) since delinked pages might reappear by different third-party URLs which make them available in through the search engines too.[223]

Reconstruction of personal memories

Memories refer the events of the past, which is basically history which include people, events, behavior, culture, act and everything. The informational revolution paved the way of unimaginable amount of memory capacity, diligence, replicability, dissemination and searchability which is in discomfort[224] with the individual privacy rights in particular, data protection right such as right to be forgotten. This phenomenon made individual data online unprecedently which is now believed to be shaping individual identities which individuals try to keep in control and represent in a self-determined way. Jonathan K. Foster (2008), clinical professor associated in Curtin University stated in his book that 'we are what we remember'[225] which means that removing information plays a pivotal role in reshaping the future since it conveys the memory from the past. So, by omitting certain events of the past, one can represent oneself as one likes which is assumed to be the gist of right to be forgotten which provides the caliber to start a new life through individual autonomy through representation. So, memories are data which are created on the basis of someone's past activities, and right to be forgotten or attempt to hiding those data also concern those data which have been recorded in the past.

Right to be forgotten advocate Mayer-Schönberger (2009) argued that ensuring a full control over personal data would empower an individual to construct their personal identity in a cherished manner such as starting a new articulated and prosperous life, a new understanding

[223] Jones, Meg Leta, Forgetting Made (Too) Easy. Communications of the ACM 58 (6), 2015, pages 34-35. (Jones 2015)
[224] Supra note 51.
[225] Foster, Jonathan K. Memory: A Very Short Introduction. London, Oxford University Press, 2008. (Foster 2008)

of oneself.[226] The matter is not only about constructing personal identity, but also the link with the past which construes the idea today while linking with the past memories of someone which creates the identity today to deal with the future. So, the real stake is the connection between past and the future.

Paul Ricoeur (1998) said in *La marque du passé* (English- the mark of the past) that each individual has an unbelievable relation with the past and the past does not prefix anyone's life to a certainty, either positive or negative, instead, it creates the forum of changing the present and the future in an inclusive way.[227] He further adds, it is a matter of individual's ability to the perception of the past which will always be related to the possibilities of the future.[228] That means our way of understanding to perceive an individual for the future is always connected to the past and that is the very essence of construing person identity. Philosophically, in order to build an inclusive and better future the reasons and motivation have to come from the past. That is why while recognizing the fact that past is inseparable, for the sake of one's story, new start of life and the reformed life, the knuckle from the past needs to be freed so that the past does not prefix or drag any reformed life in the past again.

However, Pagallo and Durante (2014), warned not to perceive past as prefixed and unchangeable always, rather, he suggested to regard it as an incomplete story which is yet to be written to make it complete, even 'revision or re-elaborations'.[229] Most historians will support that view despite removing information as this is another option to move towards an inclusive future. However, the idea of enhancing a new meaning through connecting the dots of a story might not attract desirable reactions since each new tenor needs to be accessed by the society. Additionally, as Ricoeur (1998), interpreted: the story one tries to construct is never purely oneself, it is not only 'I', rather 'we' which is based on commonly shared knowledge. That means we do not write our own stories, but there are others around us, who assist us in remembering theirs as well as ours. We frequently lend our stories from others, so do they, so it can be said that our memories are to some extent combined, not purely individual. So, there is always a connection between personal memory and combined memory and the combined

[226] Supra note 45.
[227] Ricoeur, Paul, La marque du passé, Revue de Métaphysique el de Morale 1, 1998, pages 7-31. (Ricoeur 1998)
[228] Ibid
[229] Supra note 51.

memory is likely the collection of others' personal memories. It needs to evaluate how personal and combined memories engage with each other.

Construction and reconstruction of individual and combined memories

At this point, how individual memories are connected with the collective memories will be discussed as well as the motivation of hiding any particular information will be found.

Generally, in the way of living, individuals are raised by a society where they experience undergo through a shared time and place. The most important reason of one's aspiration of representing oneself to the society is that he or she wants to interpose or bargain their position in the society as a member of it. For this reason, people want to make their present coherent with the past by being a member of the society they belong.[230] For this reason, individuals tend to reconstruct their past and try to find a motivation to expose themselves as they foment. That is why they adhere towards exercising right to be forgotten so that they are able to narrate the present through very selective realignment of the their past.[231] According to Pagallo and Durante (2014), an unfastened representation of an individual from the rest of the world is not entirely right nowadays since each reconstruction of the past has to do something with a societal task and it is solely connected with the ways and means by which societies conceptually build its own collective memories.

For the sake of understanding it better, attention needs to be focused in Reinhart Koselleck's (2004) work on 'Future's past' where the writer made a distinction between 'space of experience' and 'horizon of expectation'.[232] The former term refers to the experience of the past where an individual was walking towards the present day and the fixed footsteps that has been left behind while moving while the later is concerned with all types foreknowledge to the future which includes expectations, menace or other intentions of an individual that cast an individual down to the future which is the moment now, the 'living present'.[233] That means present or living present is likely to be understood as the bright line of the experiences of the past and the anticipation to the future and the line is stretched particularly because every past experience has the ability to drag the future anticipation in the past. That is why the individuals

[230] Ibid
[231] Ibid
[232] Reinhardt, Koselleck, Futures Past: On the Semantics of Historical Time, New York, Columbia University Press, 2004. (Reinhardt 2004)
[233] Ibid

who want to reform themselves, tend to represent or rewrite their own story by hiding past information in which they experienced their footprints through exercising right to be forgotten so that their living present is represented in a way which is consistent with the societal expectations in which they belong.

However, it is not impossible that an individual aspires to be integrated with other social groups though there is a risk of maximum semblance. Even in those situations, the hardness of unifying the forgotten faces with the datum has to be upheld so that the novelty of rebirth or fresh start could be apprehended through a meaningful data protection right. In the best possible scenarios, the reconstruction of the memories might go forward to conform with the ideas: 'space of experience' and 'horizon of expectation' jointly which means line between the two ideas remain calm and stable to make the past and the active present somehow consistent. Nietzsche (1997) opined in this regard in his Untimely Mediations that default of living is forgetting, not remembering.[234] To put it differently, living is undoubtedly possible without remembering but surely impossible if we are not allowed to forget. So, exercise of right to be forgotten can be understood as a 'plastic force' for someone which paves him or her a new way of getting rid of from the past in order to move towards a reformed life.

After analyzing the privacy interests, it can be said that one's life is not necessarily the story that solely belongs to someone. Rather identities are construed from the progression of societal relations. Experience is construed by common societal values and knowledge, and a right to a fresh start, or rebirth, or exercising right to be forgotten considers the experience of life in the past which exposes a personal identity in the living present so that the living present can be described or represented in coherence with the common shared values and expectations of the particular society today which might again be a constituent element of an individual's life past experience after some time. So, personal or individual identification is concerned with privacy interests which might be at stake. But, in essence, it is not entirely individualistic, rather, related to the society in which the individual is a member. Similarly, while individual identity is at stake, it is not limited within, it always competes with its societal identity in which personal memories are created in full. So, privacy interests are directly linked with the society in which

[234] Nietzsche, Friedrich, Untimely Mediations, Cambridge Texts in the History of Philosophy. New York: Cambridge University Press, 1997. (Nietzsche 1997)

the data subject is a member which makes the concerned data subject's privacy interests highly vulnerable.

4.2.5. Purpose achievement

It is clear from the above discussion that purpose achievement is one of the principles of putting data processing at halt. Both the further publication or further processing of a data and successful exercise to put a stop against a processing is determined on the basis of a consolidated weight of legitimate interests: publicity or privacy. The examples of publicity interests are understood freedom of expression, right to information, values of a democratic society, public interest deliberations, transparent disposal and some others, while, privacy interests proliferation include data protection, protection of fame, fresh start, protecting identity and so on.[235] While assessing a RTBF case, overall weight of the legitimate interests in particular, publication and privacy interest are weighed for the determination whether data processing will be allowed on not. The scenario is relevant here if the publication and subsequent processing of certain facts pose detrimental impact on private individual's reputation[236] viz, data related to crimes, political scandals, insolvency, or failed business attempt.

Purpose achievement essentially refers to publication purpose which is referred as achieved. Publication purpose is related to publication interest. Contrarily, putting a bar against publication or processing is connected to the privacy interests. While we are discussing about the achievement of the data publication purpose, it basically denotes the point in which the processing can be stopped. To put it differently, immediately after the data publication purpose is achieved after a certain period of time, the privacy right holders are empowered to ask for a stop processing of a particular data to hinder public accessibility. This clearly indicates that passage of time plays a crucial role in determining the point from on which the purpose of processing is achieved, and no further processing should take place in the future. According to Giovanni Sartor (2013), it is highly likely that at some point afterwards, the priority between interests shift, from publicity to privacy, to discontinue the transmission of an information[237].

[235] Supra note 51.
[236] Ibid
[237] Sartor, Giovanni, The logic of proportionality: reasoning with non-numerical magnitudes. German Law Journal 14, 2013, pages 1419-1457. (Sartor 2013)

So, now the discussion will be divided into two parts: concept of passage of time and achievement of legitimate purpose with passage of time.

4.2.6. Passage of time

The passage of time is assumed to be influencing the online data processing interests (publicity and privacy interests) in inquiring positive or negative trade-offs.[238] According to Rosen (2012), Mayer Schöenberger (2009), Koops (2011), Weber (2011) and Werro (2009), the core principle is that what was processed legitimately at an earlier stage, might be illegal, irrelevant or no longer relevant at a later time, is the very essence of digital forgetting.[239] Time lapse has something to do with approving RTBF applications. Languages used by the CJEU in *Google Spain*, by ECtHR in *Times Newspaper vs United Kingdom* cases at least indicate that clearly. During the policy proposal time in 2011, EC commissioner Viviane Reding envisioned to strengthen the RTBF within the enforcement of DPD by stating a point of time in three situations when RTBF can be exercised. According to her, an individual is entitled to find that their personal data is wiped on conditions that if the information is seized to be relevant concerning the aim for which it was obtained, or if permission of processing is revoked by the data subject or if the time limit for the processing against which the permission was obtained expires.[240] So, according to her, it involves a point of time after which further processing can be restricted and the point of time arrives after some passage of time.

The notion of passage of time is extremely fuzzy because it is a real challenge is to determine when to consider. Since while respecting RTBF, the CJEU used terms such as 'irrelevant, no longer relevant, inadequate or excessive', it is tenacious to define each of the terms by time. According to CJEU, it can be used for asking the removal of a recent data on the ground of privacy breach, again for removing distant data on the ground of irrelevancy.[241] However,

[238] Supra note 51.
[239] Supra note 26. See also, Werro, F, The right to inform v. the right to be forgotten: A transatlantic clash, Liability in the third millennium, eds. A. Colombi Ciacchi, C. Godt, P. Rott, L. j. Smith, Baden-Baden: Nomos, 2009, 285-300 (Werro 2009); Weber, R. H. The right to be forgotten: More than a Pandora's box? Journal of Intellectual Property, Information Technology and E- Commerce 2011, 2:120-130 (Weber 2011); Koops, B. J., Forgetting footprints, shunning shadows. A critical analysis of the 'right to be forgotten' in big data practice, SCRIPTed, 2011, 8:1-28 (Koops 2011); Rosen, J., The right to be forgotten, Stanford Law Review Online, 2012, 64. (Rosen 2012)
[240] Reding, V. The Upcoming Data Protection Reform for the European Union 2011. 1 International Data Privacy Law, pages 3-5. (Reding 2011)
See also, European Commission, A Comprehensive Approach on Personal Data Protection in the European Union, 2010, page 4. (EC 2010)
[241] Supra note 8, para. 92.

according to right to be forgotten scholar Victor Mayer-Schönberger, who presented right to be forgotten discussion in the most comprehensive way to date, proposed to shift from memory to forgetfulness on the basis of an expiration date.[242] The same argument is available in other scholarly opinions too which stress to implement an expiration date in particular, in cases of old and irrelevant data.[243]

The jurisdictions outside Europe for example, in Asia, Japan has been seen to be very diligent in solving matters relating to RTBF in criminal conviction cases.[244] A data subject in Japan applied to court to make Google to erase his arrest details from its search result in September 2014 which was primarily rejected by the court on the ground that the Japanese law did not vest responsibility to *Google Japan* to manage contents from its search results.[245] However, a Tokyo District Court turned the decision one month later on October by ordering Google to remove everything associated with data subject's name since it is causing real harm to the data subject by representing his past criminal activity which happened more than a decade ago.[246] While overturning another judgment decided by the Saitama District Court, the Tokyo High Court found that an accusation of child prostitution is a serious crime to the public and it continues to be momentous even after passage of five years.[247] Even in the US, which prioritized publication rights over privacy rights historically, possess a mechanism of forgiveness and erasure for criminal records.[248] The Fair Credit Reporting Act (FCRA), recognizing bankruptcy as heavier financial misdemeanor, says to remove the details of individuals bankruptcy information from consumer narration after the passage of ten years and other types of economic flux after seven years.[249] In addition, according to California State law, the driving under influence (DUI) offence records are erased after ascension of ten

[242] Supra note 45, page 198.
[243] Supra note 25.
[244] Supra note 108.
[245] Otake, Tomoko, Right to be Forgotten' on the Internet Gains Traction in Japan, JAPAN TIMES, 9 December 2014. (Otake 2014)
available at: http://www.japantimes.co.jp/news/2014/12/09/national/crime-legal/right-to-be-forgottenon-the-internet-gains-traction-in-japan/#.VkenSq6rRE5. (accessed on January 25, 2020)
[246] Japanese Court Orders Google to Halt Search Harassment, JAPAN TIMES (Oct. 10, 2014), available at http://www.japantimes.co.jp/news/2014/10/10/national/crime-legal/tokyo-court-orders-googleremove-search-results-man/#.VlO5Ka6rRE5. (accessed on January 25, 2020)
[247] Tokyo High Court Overturns Man's 'Right to be Forgotten,' JAPAN TIMES, July 13, 2016, available at: http://www.japantimes.co.jp/news/2016/07/13/national/crime-legal/tokyo-high-court-overturns-mansright-forgotten/#.V6ar2pMrJE4. (accessed on January 25, 2020)
[248] Bennett, Steven, The "Right to Be Forgotten": Reconciling EU and US Perspectives. 30 BERKELEY J. INT'L LAW, 2012, pages 161, 169. (Bennett 2012)
[249] 15 U.S.C. § 1681c (a).

years.[250] Furthermore, multiple states in the US permits adolescents to have their very selected criminal records obliterated after certain time lapse.[251] However, the US did not any machinery to accept any request for delisting URLs from search engine lists that appears on the basis of someone's name.[252] Australia has somewhat similar enactment like the US originally since 1990, which allows the qualified convicts to have their criminal records erased through 'spent conviction schemes'.[253] So, even outside the EU jurisdictions, there is hardly any specified time frame found which can be applied strictly. So, how much it really means by passage of time? After some specific time? Or at the time of applying? Or after the death of the applicant? Does passage of time always favor RTBF? Or after any other time dependent event?

The questions are highly contested, and it is difficult to answer all the questions at a time. However, Giovanni Sartor (2014) assumed and showed some of the time dependent data processing cases which comports with the contemporary development of time passage principles specified by data protection laws.

4.2.6.1. Achievement of purpose with passage of time

According to Jacobs (2015), one of the strategies for ennobling reformation is expungement of records after certain period of time which he sees as celebration though almost every Member State keeps some data for good particularly related with extremely serious offences for example, which are punishable by life sentences.[254] But most of the criminal conviction records can be considered as expungable on condition that subsequent charges have not been brought against the data subject anymore. For this purpose, the number of years can be set by the law itself. For instance, the UK has declared a term of 4 years imprisonment to set the parameter to consider certain records as non-expungable.[255] That means if any person is convicted for more than four years then according to the UK legal system, it will not consider the record as expungable ever. However, though the time span varies depending different Members' legal

[250] New DUI Reportability Requirements, California Department of Motor Vehicles, available at: https://www.dmv.ca.gov/portal/dmv/detail/pubs/dui/reportability/!ut/p/a0/04_Sj9CPykssy0xPLMnMz0vMAfGjzOK9PV1cDT3cDbzdTX0cDRy9PTz8w1zDjNwtjfULsh0VAe_Cq0o!/. (accessed on January 5, 2020)
[251] Supra note 2.
[252] Removal Policies, GOOGLE, https://support.google.com/websearch/answer/2744324 (accessed on January 8, 2020)
[253] Australian Human Rights Commission, Discrimination in Employment On The Basis Of Criminal Record; Article C, December 2004.
[254] Jacobs, James B. The Eternal Criminal Record. Cambridge, MA: Harvard University Press 2015, pages 29, 30. (Jacobs 2015)
[255] Supra note 47.

system, for most of the European countries the expungement period is generally ten years.[256] After that time the expungement should occur automatically. However, in some countries Union Member States early application for such expungement can be submitted to the relevant court such as France, Belgium and Germany.[257] In defining 'expungement' it does not refer to complete removal or demolition of the data from the record. It refers that the information is not disclosed generally anymore through any public or private communications.[258] They can only be accessed by the official authorities. However, putting concrete time frame might not be sufficient since there has been no legal instrument which specifies particular time span for each category of criminal conviction data. That is why evaluation of other processing interests are plausible.

For better understanding of processing interest and privacy interest is measured by gain and loss respectively. To make this clear, processing is gain oriented, and bar on processing due to privacy interest is loss oriented. This trend will referred as gain through processing and loss on privacy.

There is no particular time that has been defined till when a data has to be retained in particular, in case of spent criminal convicts viz, six months or couple of years after the sentence has been spent. However, there is an indication that law might take responsibility in defining the time by conferring that to an appropriate authority such as the court of law and country specific data protection authority so that they can determine whether privacy interests override the publicity or processing interests. Article 7(1) of the GDPR puts the burden of proof of processing a data on the basis of consent to the controllers to demonstrate the justification of a processing. To put it differently, data subject's position has been strengthened by making controllers responsible for showing that the processing interests outweigh privacy interests if processing is being carried out without consent because freedom to receive and distribute information exist.

An assumptive case can be drawn in which the purpose of processing is completely achieved. For example, personal information is obtained so that a lifetime one-time electromagnetic fashionable bracelet can be issued in favour of a subscriber in which his personal health data is stored. It can only be retrieved by the authorized health officials by a specific reader in cases

[256] Ibid
[257] Ibid
[258] Ibid

the subscriber (the patient in this case) is not in position to disclose his or her personal information for identification or special health situation concerns, for example, having diabetes.

4.2.6.2. Full achievement of purpose

Since data is only embedded in patient's bracelet, or in the cloud and nowhere else, in the event of losing or damaging the bracelet another one can be bought from the seller company which either recollects the data or preserves it in an encrypted form in the cloud. In this presumptive case, data collection and processing till the issuance of the bracelet is presumably allowed as the legal significance of processing for gain is present. Immediately after the bracelet has been issued in favour of the customer in exchange of consideration, further processing to the sensitive health data is not permissible since the legal significance of privacy interests seemingly overrides the commercial interest of the company towards further processing because of two reasons: firstly, further processing lacks the purpose of processing which has already been achieved which is to assign a personalized bracelet. Secondly, the further processing might have a disproportionate effect against privacy interests such as security of the information, leakage of the sensitive health data and so on. Seemingly, in this situation the loss of privacy is greater than the profit of processing. Consequently, after that point of time, any legitimate interest seizes to exist so that any can be used for the justification of any subsequent processing.

4.2.6.3. Processing after purpose is achieved

The norm is that processing of data has to be stopped imminently after attainment of purpose, though there are case where continuation of processing might be allowed. Most importantly, where the gain from processing still marginally outweighs the loss of privacy which is termed as 'continued limited processing'[259]. The CJEU confirmed this trend in the context of RTBF by confirming a data subject's having a right to be forgotten in case the retention of the data remains inconsistent with the Regulation. However, it allowed continuous processing of the same data when it is justified by law in particular for protecting the free expression right. So, the role that 'passage of time' has in continued limited processing need to be understood as the 'point of time' rather than a period of time till when the processing interest continues to

[259] Supra note 238.

override the privacy interest, even if the scale is marginally above. The further processing is barred instantly after that line crosses each other when privacy interest takes the lead and starts outweighing processing interests, *vice versa*.

For example, a person is assumed to be held liable for inciting communal violence publicly, of which video clips are also available online. The footage is relevant to be processed in the court proceedings where the accused is convicted. After his sentence is being served, the convicted person can apply for removal of the links which expose him or her to the original affairs on the ground that further processing's being not relevant or seizes to be relevant or excessive with the purposes of the processing anymore since he is a reformed criminal and it hinders his rights related to meaningful integration to the society. Besides, Sartor (2014) believes that there is an assumption that ancient data is less significant to the public and to the data subject as well since it provides little clue on a person who he or she is used to be and who is he or she now. The further processing might not be allowed since the loss to privacy comparing to the gain from processing is greater.

In addition, the applicant's full-fledged trial data is available under the judicial official authority though it is highly likely, his or her judgment is communicated to the public anonymously.

However, it might attract relevancy of processing later on if the applicant found to be involved with similar criminal activities subsequently. Again, in the question of further processing of publicly available personal data, even after the sentence is served, depends on so many other factors such as the public's having lawful interest in his or her activities, the applicant's being involved with public activities, or consulting public affairs and so on. Even if, data is kept in an encrypted non available form which can be decrypted only if it is of utmost necessity, interfering with the data in a least infringing way which might serve as the achievement of purpose[260] later on. The situation is similar in cases of newspaper archives, in which old information is preserved which are not available by conducting an ordinary search. Rather, appropriate authority has to retrieve it through appropriate reference. This is because separate archives are maintained for older data. Turning up to the bracelet case, if there becomes a need of upgradation of the device in terms of health data or the software which can be done using

[260] Sartor, Giovanni, The Right to be Forgotten: Dynamics of Privacy and Publicity, L. Floridi (ed.), Protection of Information and the Right to Privacy- A New Equilibrium? Law, Governance and Technology Series 17, Springer International Publishing Switzerland 2014. (Sartor 2014)

networks, data can be processed in a minimum scale. If it is the matter of device upgradation only, then it should be updated without committing any personal data processing at all.

The discussion indicates the possibility of continuing processing in the light of minor purposes which needs to be achieved. So, whether processing will be allowed or not after purpose is achieved is a highly contested question and there are no guarantees.

4.3. Conclusion

Clearly the principles are distinct to each other and play a different operative role in their respective domains. The initiation of application mostly starts with the determination whether a processing is lawful or unlawful. In terms of spent criminal convicts, it would not be excess to say that the controllers would put forward the journalistic expression and public interest justification in almost most of the cases. However, there are other privacy interests too which compete with the publication interests to determine a case. Privacy interests found its relevancy with the identification of specific individual and how he or she is perceived in a society. For that, values which construe their personal and collective memories are extremely important in defining their privacy violation level. Again, whether a particular privacy violation is lawful or not depends on the role of the data subject. It is evident from the *Google Spain* that in case the spent convict is an absolute public figure, the chances of removing links are almost none though the consequence might be completely opposite in the event that the spent convict or the data subject is a private figure. Lastly, the processing undertakings should be seized immediately after the purpose is achieved, however, there are certain situations when processing can be allowed even after the achievement of purpose. So, applying the principles are highly contested and completely different in each case. They need to be assessed on a case by case basis as confirmed by the highest court of the Union.

CHAPTER 5: ANALYSIS AND ANSWER TO THE MAIN RESEARCH QUESTION

5.1. Introduction

The basics and present situation of the right to be forgotten has already been discussed in the previous chapters. It is clear that it is a non-exclusive right which needs to be balanced with other contesting rights according to the balancing principles of the Union legal system. There are specific principles which regulate the operation of the right to remove any link from the Internet search results making it hard to find. However, the primary idea is that the data or information in question is not lost forever, rather, it is hard to retrieve after conducting a very general search so that the reformed spent criminal convicts are provided with a mechanism of forgiveness for their faux pas once they have committed. This surely helps them to move forward and integrate with the society. I consider the right as a privilege since it cannot be guaranteed for anyone that he or she will be awarded with an opportunity to remove their past data from online sphere. Though it can be said that the jurisprudence of right to be forgotten experienced remarkable development in the last one decade, there are still loopholes in the law which create the possibility to err against its practice. We will move to the principal research question while discussing the contemporary jurisprudence of right to be forgotten and identifying the gaps of the existing regulation in the light of previous discussions.

5.2. Findings of the Study

5.2.1. Jurisprudence of Right to Be Forgotten

5.2.1.1. Issues to be considered

In general, issues are formed on the basis of the claim of the applicant in each case. However, this section tends to discuss all relevant issues derived and identified from the previous chapters which is not necessarily complete and conclusive because there are certain issues which can be settled for all case irrespective of spent convicts only. In describing incompleteness and inconclusiveness, Bourne (2015) stated that several legitimate authorities such as different DPAs formed their own policies after the enforcement of the *Google Spain* judgment which are mostly efficient. However, it needs to be kept in mind that based on multiple reports, the

number of cases dealt by the DPAs are still very low.[261] Based on the findings of the study, one of the possible apprehensions for determining a RTBF case might attract the following issues to be resolved:

- Whether the processing qualifies its relationship with the natural person or people, and this is proven on the basis of that the information is associated with the data subject's name. However, a name is not the only thing which is necessary for the identification of a natural data subject. In that situation, if the data subject can prove that any pseudonym or other description such as house address or professional place and designation indicate the identification of the data subject, it is enough to determine that it relates to a natural person,
- Whether the data subject has any public role, or the activities related to the data subject involves the general public, or the data subject herself is a public figure. In this situation, context specific determination is necessary on case by case basis. Public's legitimate interest in data subject's activity might put a bar in exercising RTBF for example, if a crime has been committed in dispensing public performance, then it will invite public interest to know about unprofessional undertakings since it is legitimately connected with their concern,
- Whether the data is related with data subject's professional or personal life. It is important since in this undertaking, the less personal data one processing brings to light, the less attraction the RTBF would draw in any case. That means the availability of any concerned data would be fostered. Again, the issue of the data subject's being public or private personality might drag the matter either towards concealment or towards publication though even absolute public figures have the minimum privacy rights,
- Whether the concerned data of a data subject is about any criminal conviction. The public policy on exoneration of offenders and existence outside the search engines are taken into account. This situation might go mostly in favour of concealment unless the crime is recent and extremely notorious in nature. Since public safety is an issue, it has to be determined contextually on a case to case basis. Minor and older crimes with no

[261] O'hara, Kieron, Shadbolt, Nigel and Hall, Wendy, A Pragmatic Approach to the Right to Be Forgotten, Global Commission on Internet Governance, Paper Series No. 26, March 2016.
(O'hara, Shadbolt and Hall 2016)

further records of criminal activities makes the way smoother towards a RTBF or forgiveness.

5.2.1.2. Challenges in determining 'data controllers'

The application for erasing data after certain time might mean that after using of the concerned data, when there is no relevancy of the data anymore, or after elapsing crime specific time, when the detriment to privacy rights outweighs the benefits or advantages of publication or further processing rights, the data subject can ask or request for the removal of the data or identical elements from the data. Undoubtedly, if the data is not relevant, or inaccurate or on the basis of any other justified objection, the data subjects have the right to see the data to be removed from the search engine list under Art. 17(1) of the GDPR. According to law, this right is essentially invoked against the data controllers (natural, or legal or public, or private entity who jointly with others determine the purposes and the ways of personal data processing)[262]. Nowadays it is generally the public and private entities for example, who are connected in Web 2.0 application systems.[263]

The concept and definition of controller was relatively easier at the dawn of emerging the Internet. But now in today's user centric informational processing era it is highly complicated for different role players. For example, in cases of mobile devices, the network and application providers are the data controllers which should erase all data after a certain holding period in accordance with law.[264] The same goes with the CCTV video data. Besides, in cases of personal third party undertakings for example, blogs and other photos and videos, where being a third party, the data controller is processing data of the data subject, the situation is different since social networking services (SNS) are involved in which the user is the controller of own posts and blogs who can delete or preserve at will. However, according to Article 29 Working Party opinion, SNS service providers are the data controllers since they principally ordain the purposes and ways of processing.[265] However, it is also true that the users of such SNS service networks are also the data controllers on condition that their activities are not associated with the 'household exception'.[266] The household exception exempts an user to qualify as data

[262] Article 4(7), GDPR
[263] Koops, B. J., Forgetting footprints, shunning shadows. A critical analysis of the 'right to be forgotten' in big data practice, SCRIPTed, 2011, 8:1-28, page 237. (Koops 2011)
[264] Directive 2006/24/EC.
[265] Article 29 Data Protection Working Party, Opinion 1/2010 on the Concepts of "Controller" and "Processor" (2010), at 21.
[266] Ibid

controller on the grounds that the user of SNS service performs on behalf of a commercial establishment such as companies or associations, or performs with an objective connected to political and charitable motives.[267]

Apparently, there might be two situations when data processing is related with using SNS services. Firstly, the data subject is himself or herself the data user, and secondly, third party is the controller. In the former case, the data subject can remove or erase the data so easily at their convenience though according to Article 29 working party opinion, the SNS forum providers such as newspaper archives, YouTube or Facebook or other blog host websites are also data controllers. In that case, user can ask the provider to delete or remove the data. However, in the latter case, when third parties are simultaneously the users and the data controllers. They can be among friends and families, or other legal or natural person. In that case the data subject can request the controller to have the data removed or even the SNS service provider who is in position to remove or erase from its network systems.

So, from the above discussion, it is clear that a request for having a data deleted needs to be submitted to the data controllers. To put it differently, the data controllers have not only the primary responsibility of determining the aims and means of personal data processing, but also to decide what to do with a RTBF issue in question. However, inconvenience shows up if the data controller appears to be a third party who falls within the so-called household exception. In reality, it might be difficult to point out the right data controller to whom the erasure request can be submitted though it appears to be so convenient in theory.

5.2.1.3. Reason and time intertwine while seeking a right to be forgotten

The first and foremost reason for invoking a RTBF is the retention of data which pose a specific detrimental effect to individual's privacy and reputation.[268] It can be interpreted to have two derived contexts: 1. The preservation of the data is causing detriment to the data subject now in the present and existing situation, and 2. The data's being no longer necessary for any of the purposes and so their preservation may have a detrimental effect to the data subject at any point in the future.

[267] Article 29 WP, Opinion 5/2009 on Online Social Networking, 2009, page 6.
[268] Supra note 263, page 240.

The first situation is comparatively frank and related to Art. 17 of the GDPR which states about having a right to erasure. According to Art. 17(1):

> ''The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay…''

However, this claim is of course conditional not unfettered.[269] Again any objection neither seek nor qualify as a complaint against all types of processing activities, *inter alia*, collection, usage, retrieval, publication, modification and so on. It can be limited with only one type of processing for example, the claimant can ask or the data controller can argue that an objection or request is justified with regard to storage or dissemination only but not on collection, or retrieval which indicates that there is a possibility of emerging the respective content in the future.[270] In that situation, the data subject has to request the removals over and over again in the future.

The possibility of having negative effects in the future is the second reason of requesting the removal of an information. The GDPR rightly perceived the risks in its provisions by requiring the controllers of a data not to be obliged to include identification data of the data subjects in cases when the purpose of the processing does not demand the identity of the data subject. In one of the data principles, the GDPR states in its Art 11(1):

> ''If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject…''

If in accordance with Koops (2011), a 'generous data subject friendly' interpretation is applied here, then it can be said generally that a request for erasure can be submitted against any processing which is deemed to have been processed unlawfully. However, a less data subject friendly interpretation is also possible, in that case, the application will solely relate particularly to the existing incorrect data only[271] because at the least, every data subject has *prima facie* legitimate interest in having insights into probable detrimental data to be forgotten before it actually harms. Though it is also true that there are other legal remedies to be sought against

[269] Under Art. 17(3), GDPR
[270] Supra note 268.
[271] Ibid, page 241.

other similar right violations which can be adhered in particular, for example, remedy against defamation, in all scenarios the data subjects are in tough position to show the controllers or the court of law that the harm caused by the processing, outweighs the gain obtained by processing. However, it needs to be distinguished that law relating to defamation facilitates recourse with regard to false detrimental publications, while a RTBF for the spent criminal convicts mainly provides recourse against accessing true information from the public gaze.[272]

That is why the probable harm in the future is not surprising and a claim for removal of data on the grounds of already no longer relevant, to put a stop on the data from lagging around and emerge immediately in a time when the risk of harming privacy rights at the peak.

According to Art 25(1) of GDPR, which states about protecting data by design and default, the data controllers are required to put forward exact 'technological and organizational' steps such as 'pseudonymization' and 'data minimization' both at the time of fixing the purpose and for further processing to comply with other data protection principles.

Again, in terms of storage of data is apprehended for 'historical, statistical or scientific research purposes' under Article 83, the data controllers will take necessary safeguards for those data which includes that data controllers will delete data immediately after the usage is done or anonymize or minimize in other way to comply with the data processing principles to meet the same end to meet particular right to be forgotten.[273] This will eventually foster minimization of the risk which is also possible during legitimate processing of data. However, it has to be kept in mind that the controversies in argument occurs particularly when the data in question is retained for longer period than allowed which put the data subject into greater risk of unwarranted processing as well as exposure.

5.2.2. Gaps of law still needs to be filled

In order to describe the ways on how the right can be implemented, it is necessary to identify the loopholes of current data protection law in spent criminal convicts:

[272] Grant v. Torstar Corp., 2009 SCC 61, at para. 59.
[273] Hildebrandt, M. Profiling and the Identity of the European citizen, M Hildebrandt and S Gutwirth (eds), Profiling the European Citizen, Springer, 2008, pages 303-326. (Hildebrandt 2008)

- There is a lack of regulation in case of user's 'household exception' for publishing contents about the criminal convicts in social networking platforms,
- The criminal convicts must be empowered for requesting a stop on the processing even during the permitted processing period, since it needs to be perceived as a mere request for stopping further processing which lies within the ambit of right to be forgotten, and it is additional and different from erasure or delink information,
- The obligation of minimizing the data to the controllers surely leaves room for exercising vast and opaque discretionary power to define the scope of secondary, minor or other compelling purposes which might end up in longer retention of personal data since the controllers have legitimate business interest which necessarily err to lengthier retention period,
- An application criterion for a right to erasure should be broader expanding from Art. 17(1) to the all circumstances when the concerned data appears to be inaccurate or incomplete and data is being processed for purposes related to 'functional creep',
- The law does not entail any specific period on how long a data is allowed to continue processing, rather, it leaves the responsibility on the data controllers with a wide scope of expounding other purposes. However, it needs to be mentioned that multiple areas of laws are already pertaining forgiveness through social forgetfulness, for example, in bankruptcy, adopting reformatory measures for juvenile delinquency, and fixing a time limit on retaining credit history.[274] And the trend of forgiveness can also be expanded in other areas such as consumer law, labour, and administrative law. Thus, preventive criminal justice apprehension actually can have an impact on outlining guidelines on how privileged groups can behave with data related to under privileged groups.[275] This is essentially the elements of a right to clean slate or forgiveness, not erasing anything for good.

It is appearing that there are considerable gaps in the current data protection regulatory system which might undermine the full achievement of existing jurisprudence. Policies and enforcement on behalf of the data protection authorities in terms of powers and competences are in crying need. Nowadays, emphasis is put mostly on data protection by default through design and it well comports with the current regulation as well under Art. 25 of the GDPR.

[274] Supra note 25.
[275] Koops, B.J. Law, Technology, and Shifting Power Relations. 25 Berkeley Technology Law Journal, 2010, pages 973-1035. (Koops 2010)

Many scholars support the approach for tackling the implementation difficulties through applying technical enforcements in place.[276] However, assessing data protection by design possibilities and mechanisms in case of the spent convicts are not the subject matters of this paper.

5.3. Answer to the primary research question

This primary purpose of this paper is to inquire into the issue that whether RTBF can be guaranteed in the cases of spent criminal convicts. To have a possible answer to that presumption; a broad analysis on the requirements of right to be forgotten, the balancing approaches of the right with other fundamental competing rights with special reference to right to freedom of expression, and the ways and means of the application of identified principles are apprehended in the previous chapters respectively.

First of all, the concept of 'right to be forgotten' or 'right to erasure' does not attract a literal interpretation while defining it since it essentially does not refer to something amounted to be deleted or removed permanently, but to eliminate the traces which link with the search engines to make the retrieval easier. So, the primary concept and purpose of right to be forgotten is related to hiding or making retrieval hard by severing the link between the search engines and the third-party data hosting websites. In practice, the data stays where it was published *prima facie,* but it is not retrievable unless knowing the exact source which is amounted to narrowing the accessibility. In that way the data subjects which are here the convicts who already spent their convictions are helped to hide their conviction data to have further negative repercussions in their personal lives with the aim of helping them to start a new beginning in their lives. The complications are heavier online since the emergence of Web 2.0 facilitated unimaginable data storage and retrieval capacity in which anyone has access to the informational superhighway can be processor of those data which makes not only complex but also difficult to put a stop in further disseminating.

Secondly, the age of personal data protection mechanism is couple of decades old but the modern right to be forgotten is being developed as an aspect of personal data protection or a privacy right for merely a decade. It is clear from the data protection law as well as the case laws from the CJEU and the ECtHR that the right to be forgotten has certain limitations which

[276] Cavoukian, A. Privacy by Design: The Definitive Workshop. A Foreword. 3 Identity in the Information Society 2010, pages 247-251. (Cavoukian 2010)

make the right non-exclusive in nature. According to CJEU, when a processing is considered as inadequate, inaccurate or no longer relevant with regard to the purpose of processing, and such processing contains such personal data which unveils an individual, the data needs to be deindexed from the search lists. According to the data protection law, a processing has to be done in accordance with the data protection principles under chapter II of the GDPR. If that is not in accordance with the law, then the data subjects can ask for a so-called removal of that data under Art 17(1) of the GDPR. However, there are certain bars mentioned in Art 17(3) which can deter data subjects from exercising a RTBF among which the most controversial is that the publication right named right to freedom of expression and of the press, a well-established legal right under Union jurisdiction. Since the scope of the latter right extends to receive and dissemination of information, balancing this public right with privacy right of to be forgotten is inevitable.

Balancing between rights is one of the principles of the Union legal system driven by the principle of proportional effect. Since the *Google Spain* ruling, balancing is adhered between RTBF and free expression. It is established from the judgment that in cases the information related to the criminal records are lawfully published or processed then rationally public's right to access to that information will be upheld. Though under Art. 10 of the GDPR, the criminal conviction data is considered to be processed only under the official authority, the necessity of journalism to convey a message to the concerned public who has legitimate interest cannot be underestimated. Besides, historians tend to study renowned figures, or define a criminal trend by analyzing statistics comprise of certain types of offences scientifically. For them, the internet archives are one of the most convenient sources to have insights of data. However, the criminal records can be found without any hint which can unveil spent criminals to the direct societal gaze. For this, data minimization principle can easily be adhered which is used by pseudonymizing the data subject so that he or she remains under cover. But in the event of the data subject's being a public personality in whom the common people naturally feel the interest of knowing about their perpetration, data minimization rule might not be allowed so that the common people can have an insight in matters which involve public security. That is highly connected with professional omissions since in cases of omissions while performing any responsibility of trust, the faux pas is considered important and relevant to be published widely irrespective of considering any public or private figure. The purpose of processing plays a very important role in this perspective. If the purpose is to let people know something they are entitled know, then the chance of controversies is diminished. That is why even the absolute

public figures such as politicians, higher public officials, ministers or other celebrities do enjoy some level of privacy since the purpose of publishing any concerned data needs to be taken into account in each case differently and contextually so that unlawful processing can be prevented. For instance, considering the nature of the crime and the context, the court held that the publication of the facts was physically fair, natural and accurate.[277] However, in case of NT2, the court stated that invading into official's employees' privacy with the objective of finding mischievous actors, is not regarded as an act of dishonesty, rather in good faith[278] and consequently NT2 obtained an order of delisting.[279]

So, in balancing between privacy and publicity rights such as right to be forgotten and freedom of expression, both have its own justifications and limitations. Though previously, due to the legal nature of Directive, depending on Union jurisdictions, there was a possibility of differing balancing mechanisms greatly, but now the mechanism has been and being unified after the enforcement of the Regulation. That is why specific principles are inevitable to emerge as a part of Union legal system which can be applied in deciding RTBF cases in terms of the spent criminal convicts in particular to decide which one would be upheld: right to freedom of expression or right to be forgotten.

In assessing the ways and means of applying the above-mentioned principles in the case of reformed spent convicts' right to be forgotten, the comprehensive discussion of previous chapter sheds light on the inherent characteristics of the principles. There are considerable number of elements which need to be taken into account while deciding and prioritizing the principles one by one namely among, lawful and unlawful processing, public and legitimate interest, public and private figures, processing and personal interests, purpose achievement and passage of time.

Now, turning into answering the main research question, whether a RTBF can be guaranteed to those who spent their felonious convictions or not. The answer undoubtedly is 'no'. There are no guarantees that a spent criminal convict will be awarded with a decision that enables them to get rid of their past every time. Every case starts with framing the competing issues to be resolved and the facts resolve around the law and related jurisprudence. After considering the elements competing principles, it is possible to reach to a decision on whether a processing

[277] NT1 and NT2 v Google and The Information Commissioner**,** [2018] EWHC 799 (QB), at 157.
[278] Ibid, at 222.
[279] Ibid, at 227, 228, 230.

is lawful or unlawful. That means the claimant, or the data subject is allowed to apply for a right to be forgotten but it essentially has to confront the possibility of rejection.

5.4. Conclusion.

According to Victor Mayer-Schönberger, an Oxford professor, humans were excellent in forgetting than remembering before the age of Internet. That is why he suggests that we should focus more on forgetting rather than remembering now. Now the humans are more accurate and defensive in informational storage since registration, storage, availability and retrieval are peaking in every possible way through the advancement of communication technology. However, the protection of data online could not keep pace with the technological advancement. That is why Victor Mayer further suggested to have a pragmatic mechanism to memorize few. Memorizing few essentially does not mean that we are required to input less data in the permanent storage, but to make how hard it is to retrieve or find an information. For this, the focus should be on how the data can be found unlike previous when the focus was how data is retained.

Technological advancement shaped a world where society has to acquire the knowledge of forgiveness since forgetting is not the norm anymore. Since forgetting is an indispensable part of human lives, the practice of forgiveness has to be cultured because forgiveness helps to forget.[280] That is why if the world stops itself to forget anything, it will eventually destroy any chance for anyone for reformation and moving forward.[281] At this point, it is already established that there is a line between public's legitimate and illegitimate right to access an information. If societies enact laws with the objective of affording a spent convict to move on with his or her life without frontiers, then it must also reflect online. The right to be forgotten can play the role to be the front liner for helping people in reformation.

From the existing demonstration of the right, it is clear that there is no security that the right will be granted anytime requested. But one of the most important features is the right can be implemented without violating other fundamental rights. Though it still did not get the status of an internationally recognized right, but in the near future remarkable territories should adhere to it inevitably for a healthier and more humane society.

[280] Douglas, Michael, Do We Have The Right To Be Forgotten? 6:10 TED (2015), available at: http://tedxtalks.ted.com/video/Do-we-have-the-right-to-be-forg (Douglas 2015)
[281] Supra note 108.